US005970149A

United States Patent [19]

Johnson

[11] Patent Number: 5,970,149

[45] Date of Patent: *Oct. 19, 1999

[54] COMBINED REMOTE ACCESS AND SECURITY SYSTEM

[76] Inventor: **R. Brent Johnson**, 10816 E. Newton St., Tulsa, Okla. 74116

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/892,982**

[22] Filed: **Jul. 15, 1997**

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/752,249, Nov. 19, 1996.

[51] **Int. Cl.**[6] **G06F 11/00**; H04L 9/00; H04K 1/00

[52] **U.S. Cl.** **380/49**; 380/2; 380/21; 395/183.22; 395/185.1

[58] **Field of Search** 380/2, 21, 49; 395/183.22, 184.01, 185.1, 200.54, 186, 187.01, 188.01

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,182,933	1/1980	Rosenblum	380/21
4,310,720	1/1982	Check, Jr.	178/22.08
4,430,728	2/1984	Beitel et al.	364/900
4,531,023	7/1985	Levine	179/2
4,578,531	3/1986	Everhart et al.	380/21
4,763,351	8/1988	Lipscher et al.	379/95
4,965,804	10/1990	Trbovich et al.	380/21
5,179,695	1/1993	Derr et al.	395/183.07
5,204,961	4/1993	Barlow	395/725
5,237,677	8/1993	Hirosawa et al.	395/185.1
5,347,578	9/1994	Duxbury	380/4
5,416,842	5/1995	Aziz	380/30
5,452,460	9/1995	Distelberg et al.	395/700
5,537,554	7/1996	Motoyama	395/183.22 X
5,550,984	8/1996	Gelb	395/200
5,678,002	10/1997	Fawcett et al.	395/183.01
5,854,828	12/1998	Kocis et al.	379/93.317

FOREIGN PATENT DOCUMENTS

0474058A2 3/1992 European Pat. Off. G06F 11/00

OTHER PUBLICATIONS

Hamish Butler, "Virtual Remote: the centralized expert.", Hewlett-Packard Journal Oct. 1994.

"New PC: IBM redefines Home Computing with breakthrough split system design . . . " Edge Work-Group Computing Report, V7, p. 10, Sep. 30, 1996.

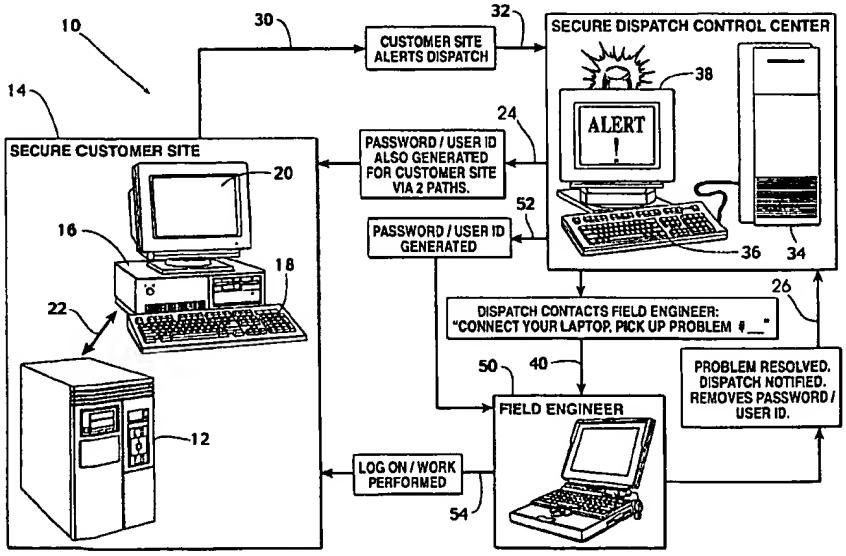
Primary Examiner—Pinchus M. Laufer

Attorney, Agent, or Firm—Head, Johnson & Kachigian

[57] ABSTRACT

A combined remote access and security system for servicing a secure mainframe central processing unit having a console monitor. A secure dispatch central processing unit for receiving problem reports concerning the mainframe central processing unit is in communication with the console monitor. A field engineer's central processing unit is in communication with the dispatch central processing unit. A data encryption key is randomly generated and transmitted from the dispatch central processing unit to both the field engineer's central processing unit and the console monitor. The field engineer central processing unit is in communication with the mainframe central processing unit wherein data transmitted from the field engineer's central processing unit is encrypted and wherein the encrypted data is decrypted at the mainframe console monitor.

12 Claims, 15 Drawing Sheets



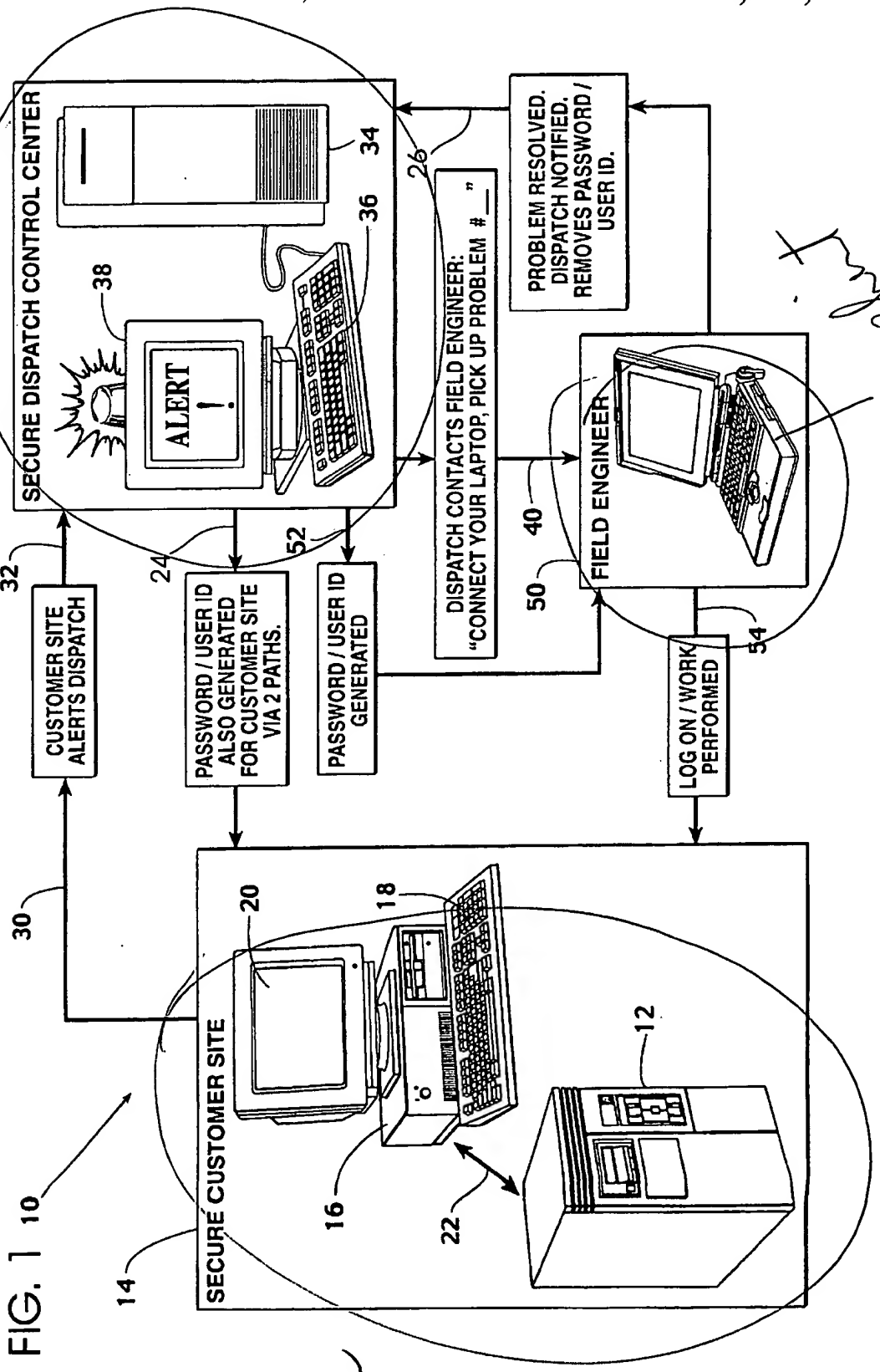

SECURE DISPATCH CONTROL CENTER
ALERT
!
34
36
38
26
PROBLEM RESOLVED. DISPATCH NOTIFIED. REMOVES PASSWORD / USER ID.
DISPATCH CONTACTS FIELD ENGINEER: "CONNECT YOUR LAPTOP, PICK UP PROBLEM #__"
FIELD ENGINEER
40
50
54
52
24
32
CUSTOMER SITE ALERTS DISPATCH
PASSWORD / USER ID ALSO GENERATED FOR CUSTOMER SITE VIA 2 PATHS.
PASSWORD / USER ID GENERATED
LOG ON / WORK PERFORMED
30
SECURE CUSTOMER SITE
20
18
12
16
22
14
10

FIG. 1

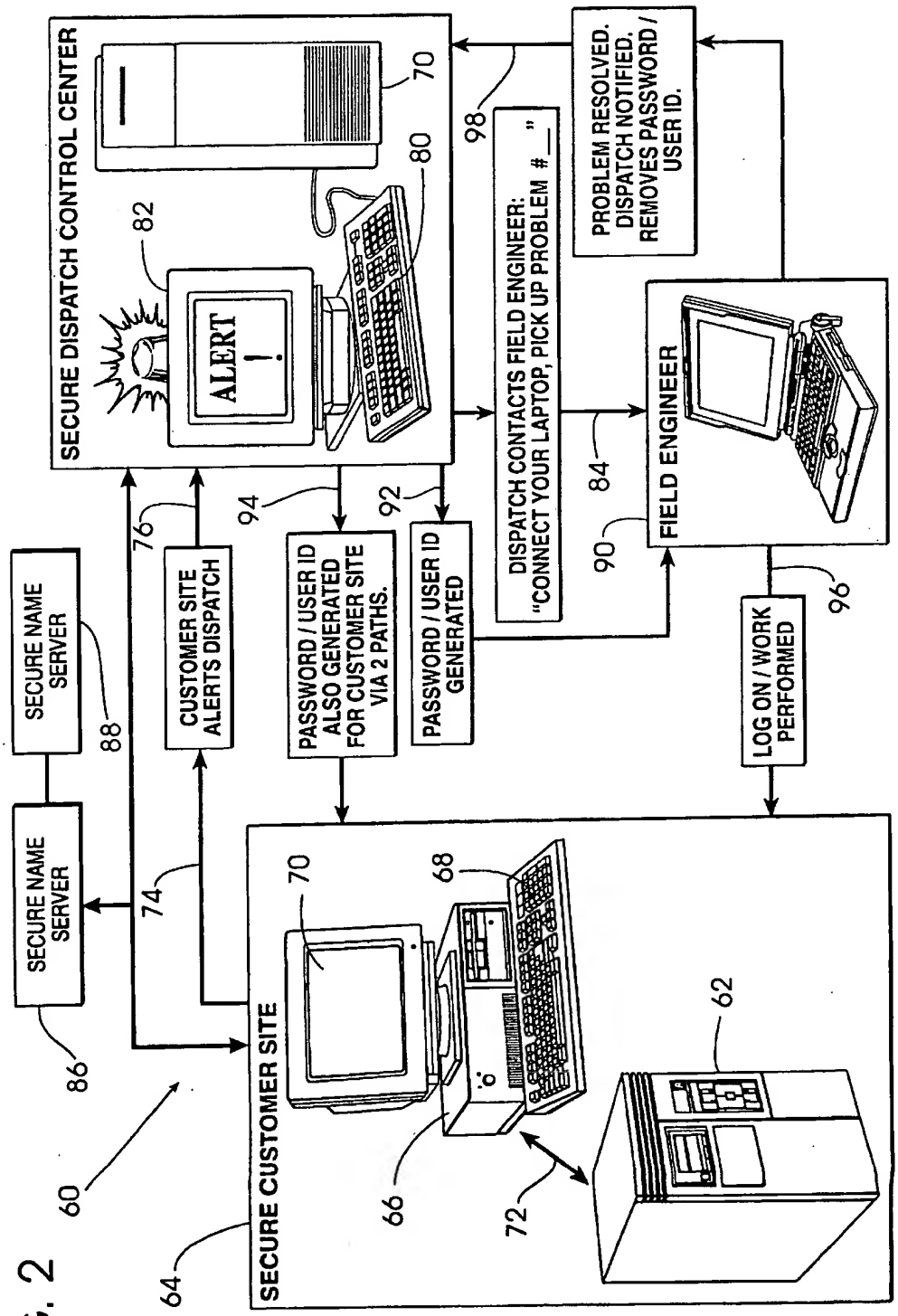

SECURE DISPATCH CONTROL CENTER
ALERT !
70
80
82
98
PROBLEM RESOLVED. DISPATCH NOTIFIED. REMOVES PASSWORD / USER ID.
DISPATCH CONTACTS FIELD ENGINEER: "CONNECT YOUR LAPTOP, PICK UP PROBLEM #___"
FIELD ENGINEER
84
90
96
LOG ON / WORK PERFORMED
PASSWORD / USER ID GENERATED
PASSWORD / USER ID ALSO GENERATED FOR CUSTOMER SITE VIA 2 PATHS.
92
94
76
CUSTOMER SITE ALERTS DISPATCH
SECURE NAME SERVER
88
SECURE NAME SERVER
86
74
SECURE CUSTOMER SITE
70
68
62
66
72
64
60

FIG. 2

Process at Customer Site Monitoring for Alerts FIG. 3A

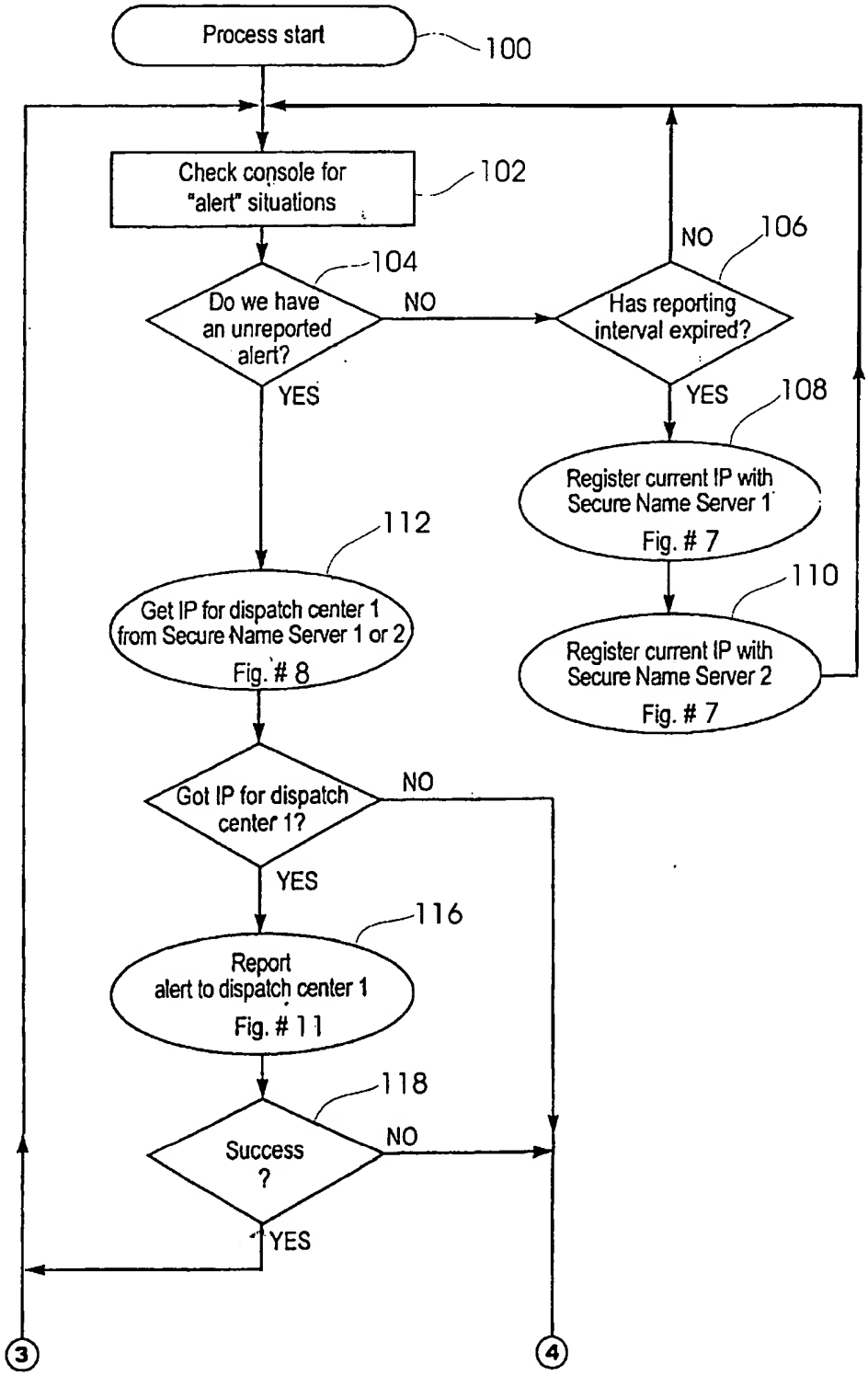
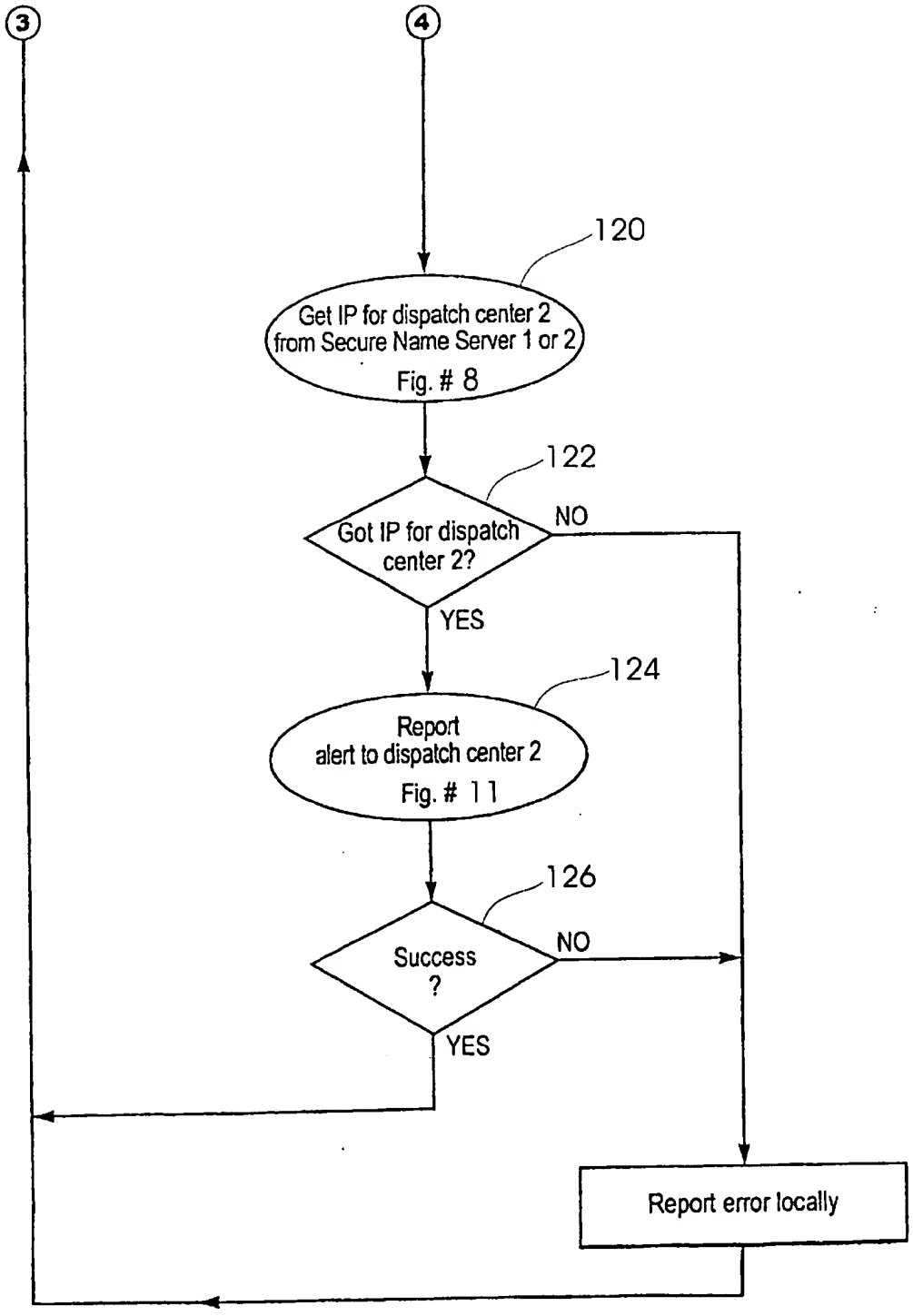
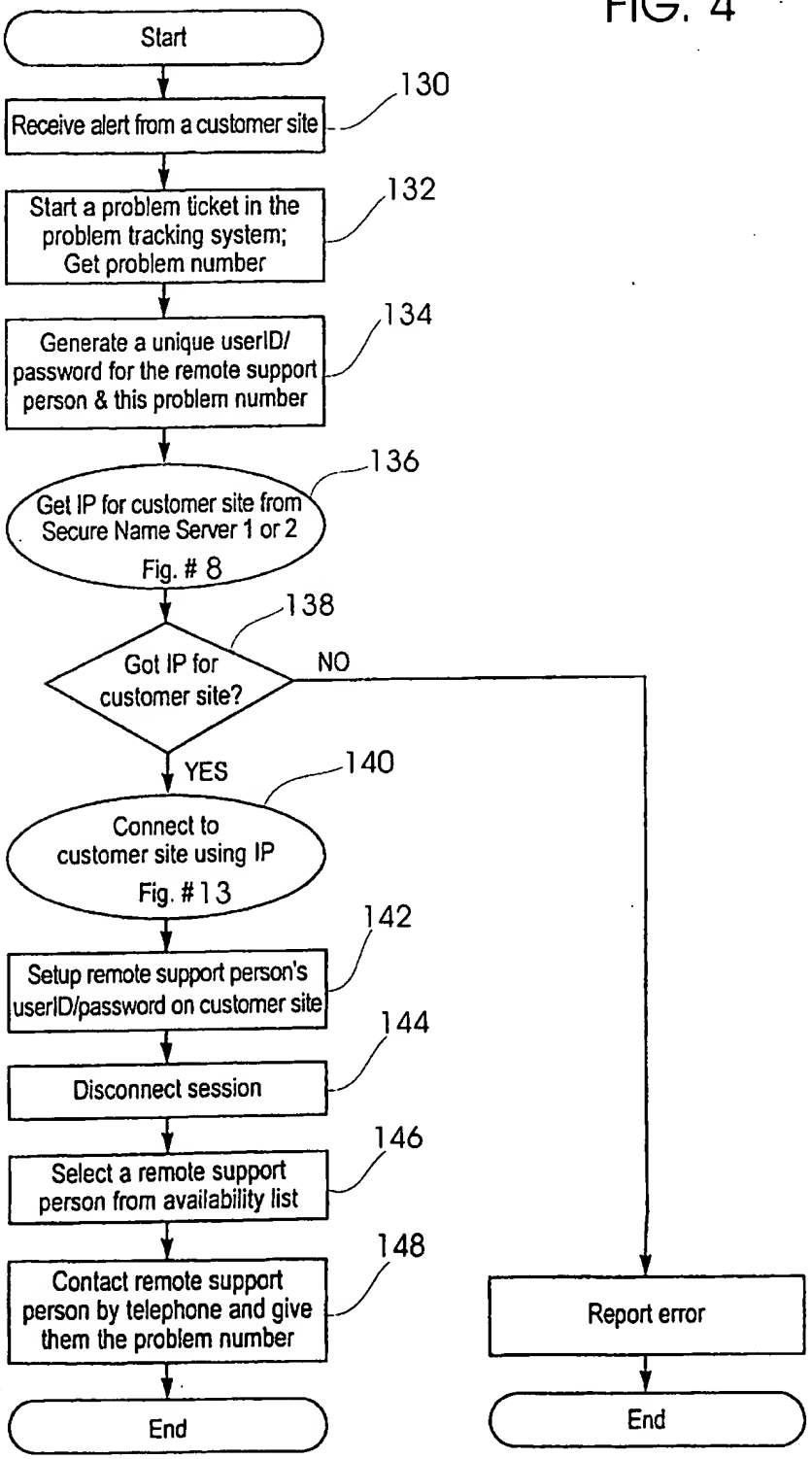


FIG. 3B


3
4
120
Get IP for dispatch center 2 from Secure Name Server 1 or 2
Fig. # 8
122
Got IP for dispatch center 2?
NO
YES
124
Report alert to dispatch center 2
Fig. # 11
126
Success ?
NO
YES
Report error locally

Dispatch Center Handling an Incoming Alert from a Customer Site

FIG. 4



Process Remote Support Person Follows to Handle Problem Reports

FIG. 5A

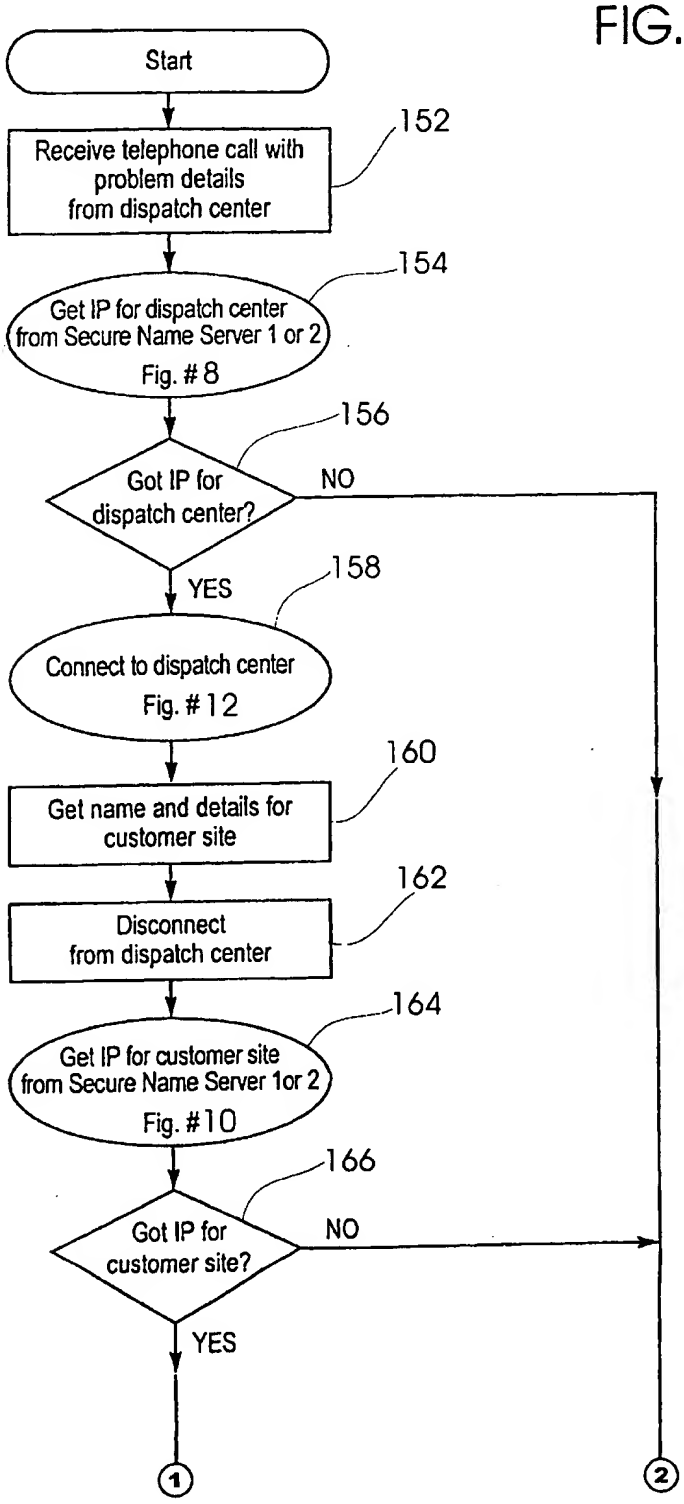
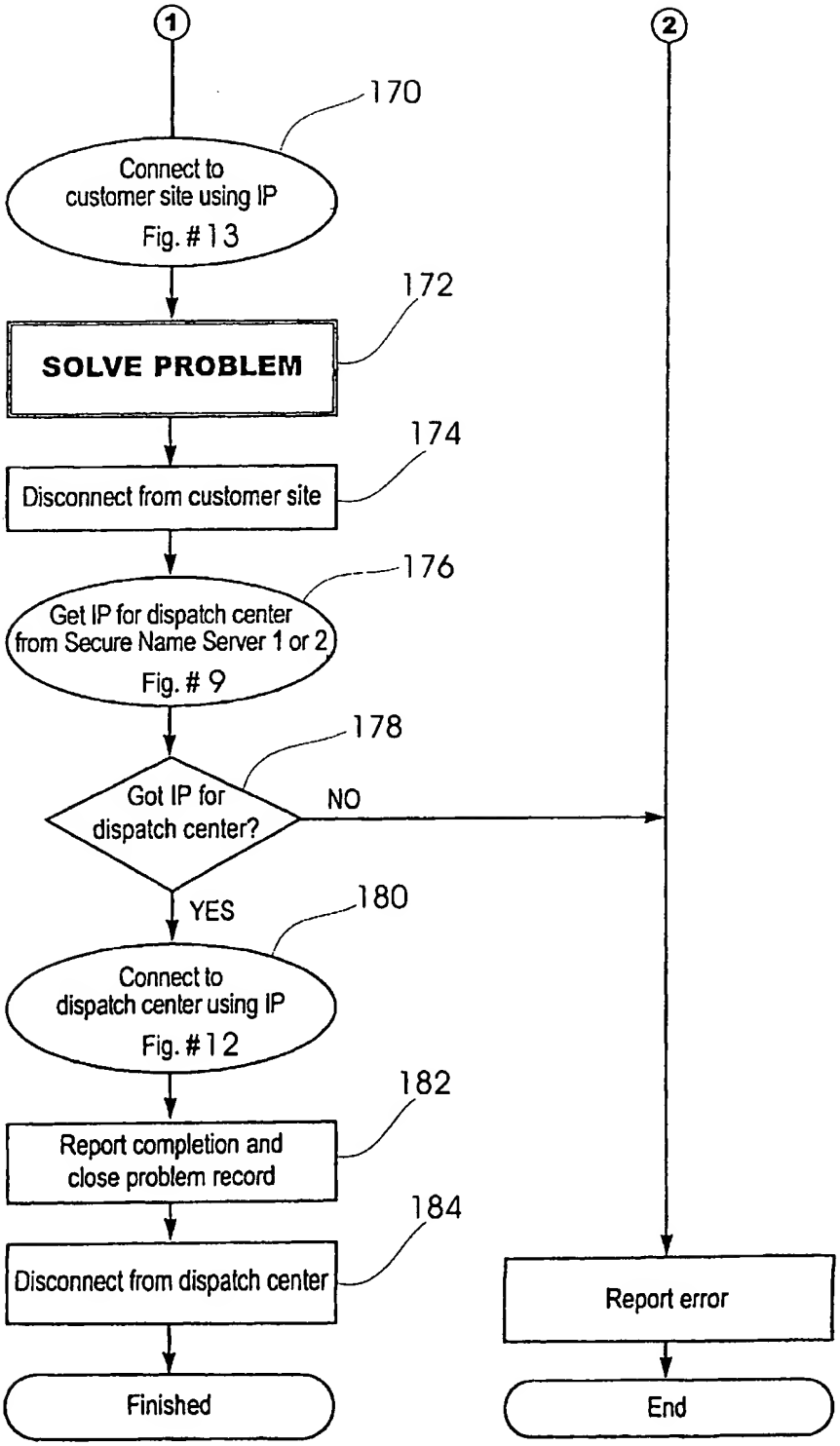


FIG. 5B


1
2
170
Connect to customer site using IP
Fig. #13
172
SOLVE PROBLEM
174
Disconnect from customer site
176
Get IP for dispatch center from Secure Name Server 1 or 2
Fig. # 9
178
Got IP for dispatch center?
NO
YES
180
Connect to dispatch center using IP
Fig. #12
182
Report completion and close problem record
184
Disconnect from dispatch center
Finished
Report error
End

Dispatch Center Invalidating Remote Support Person's Password at Customer Site

FIG. 6

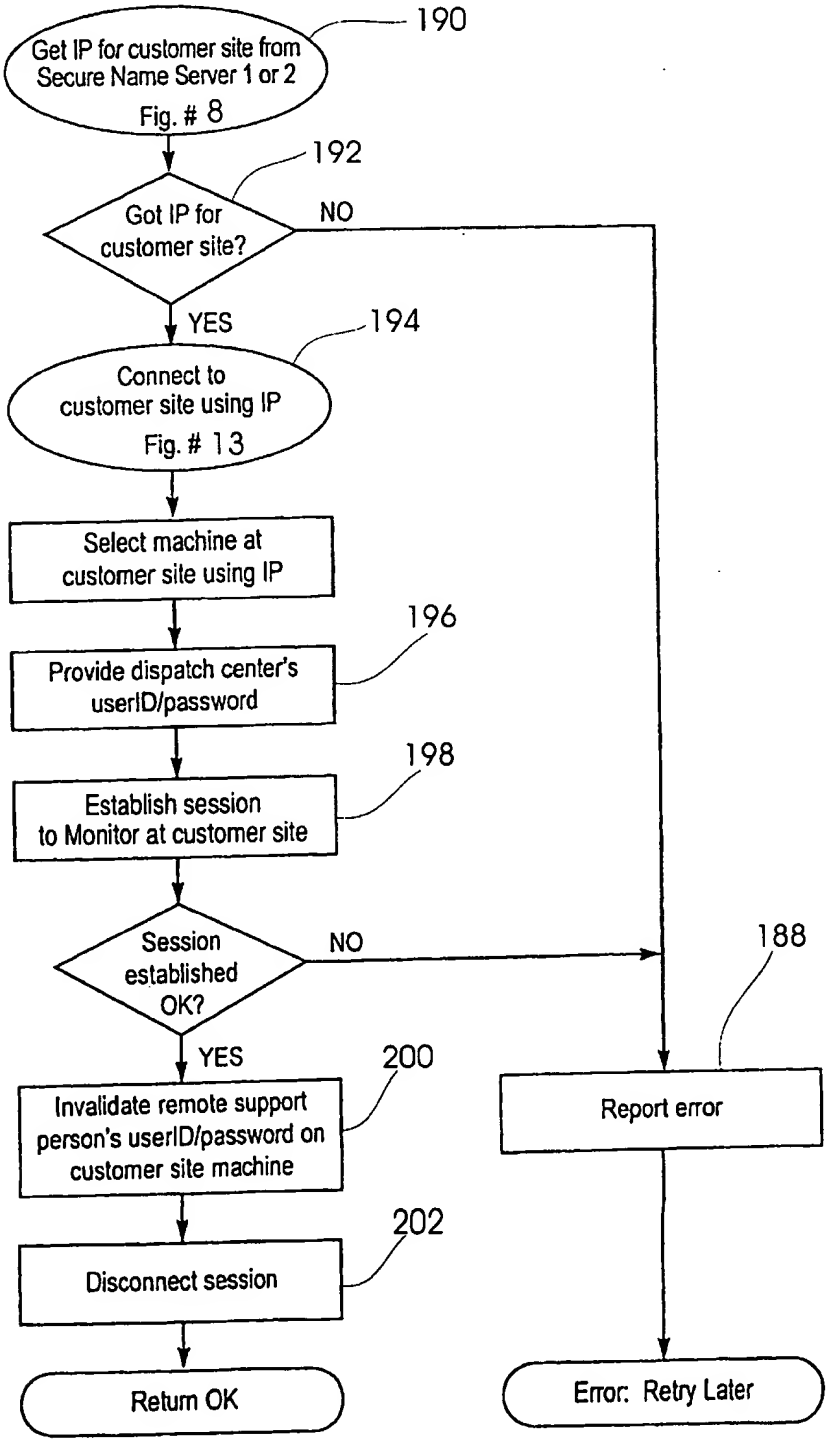
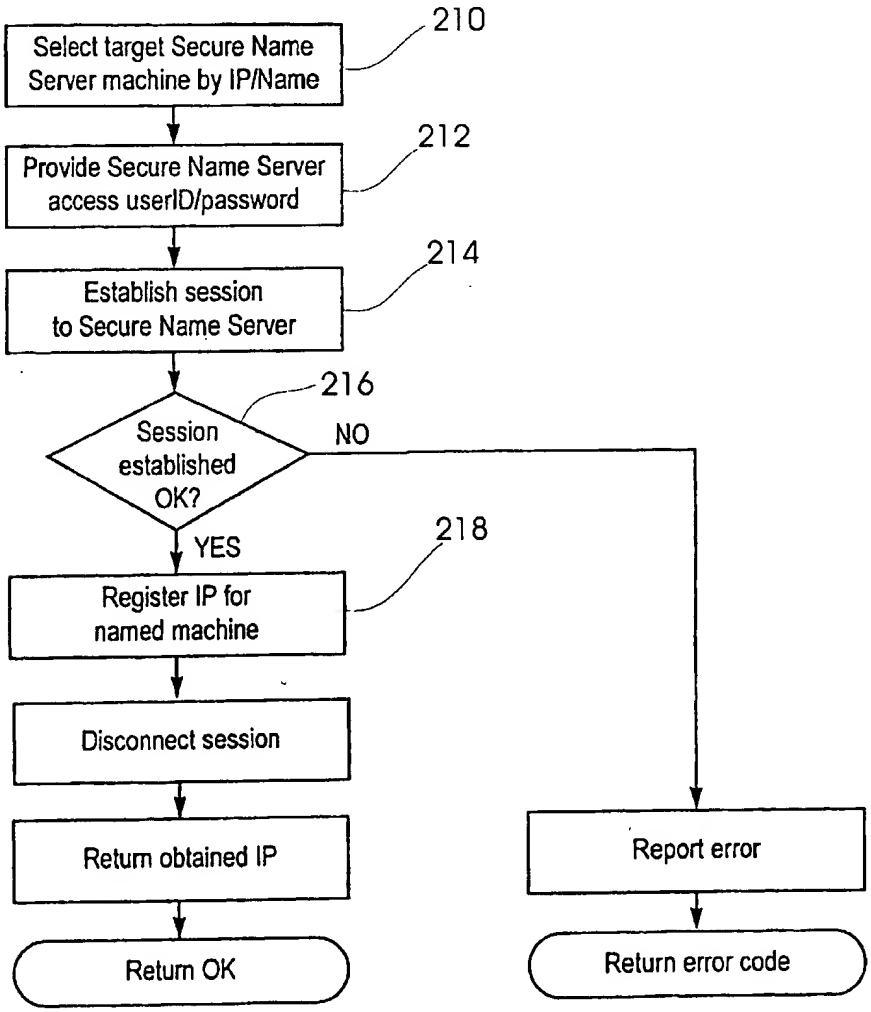


FIG. 7

Process to Register Machine with a Secure Name Server



Process to Get an IP from a Secure Name Server

FIG. 8

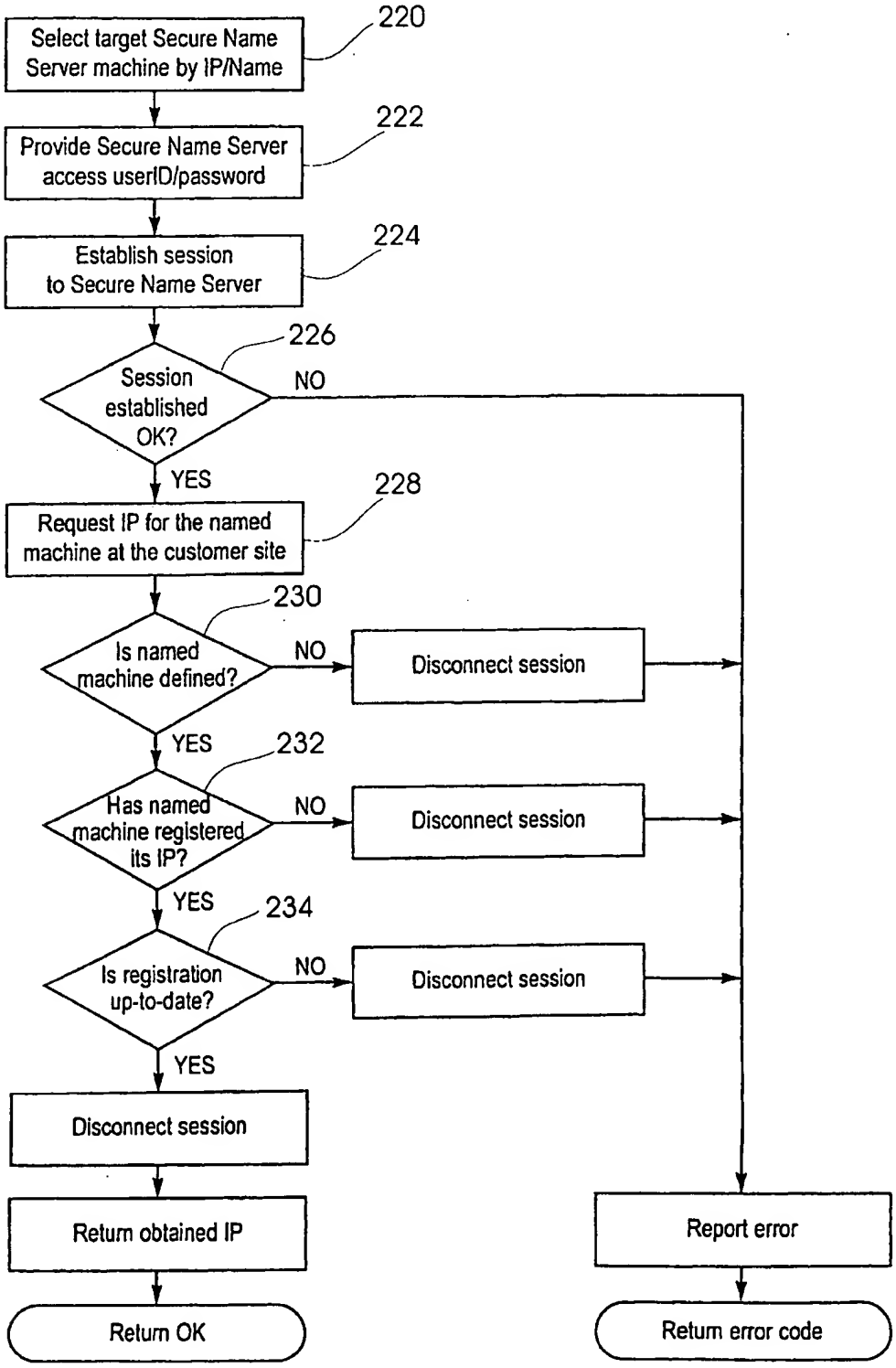


FIG. 9

Process to Obtain an IP Address from Secure Name Server 1 or Secure Name Server 2 for Dispatch Center

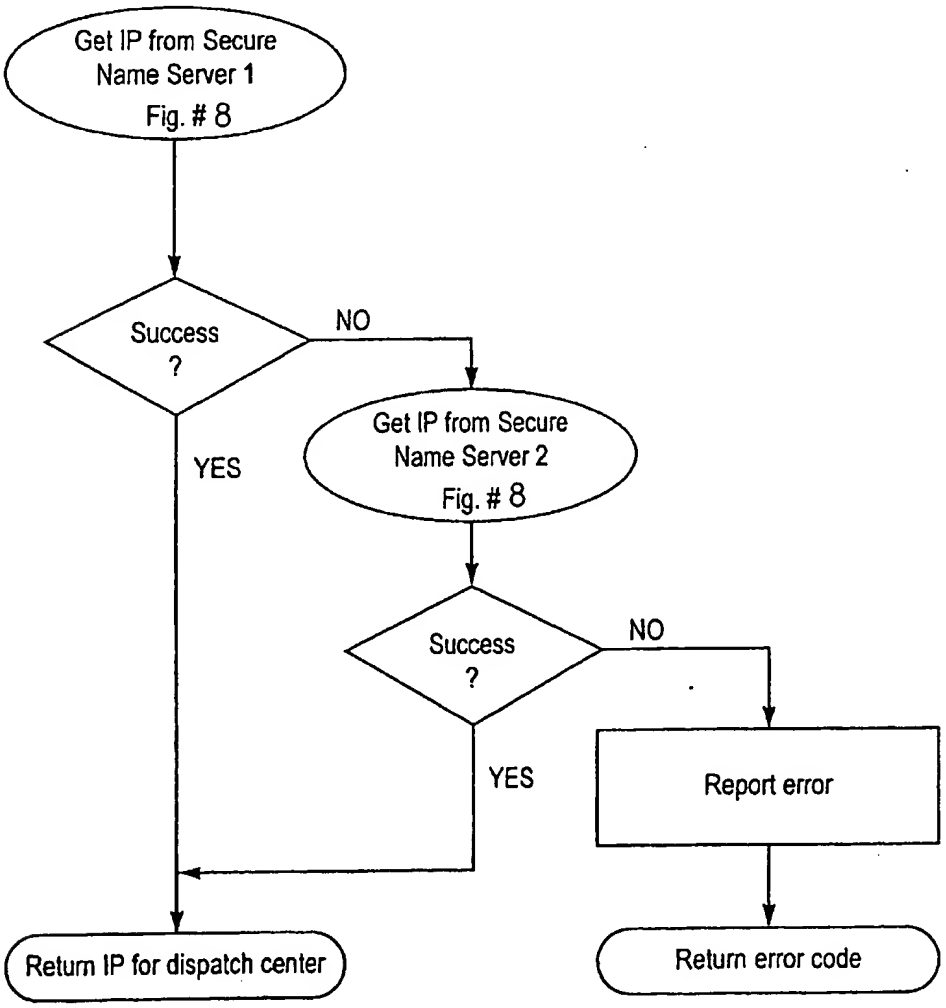
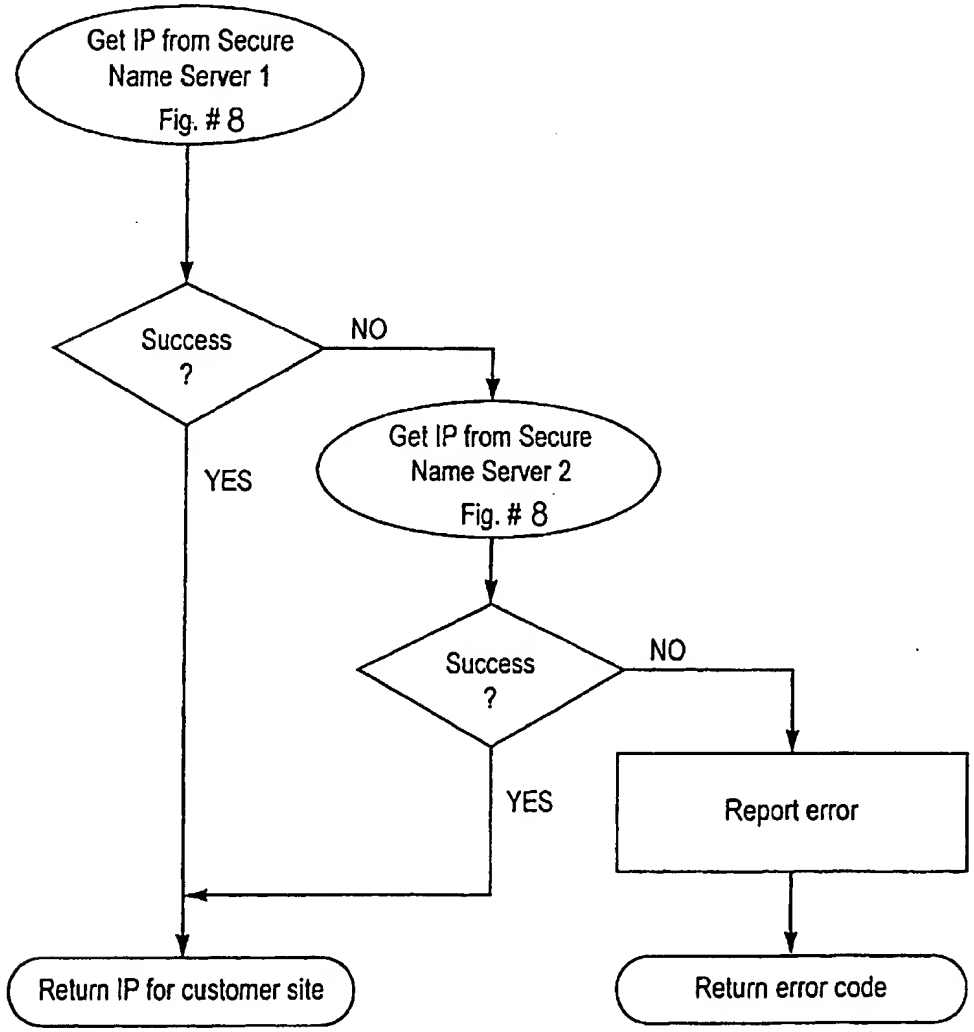
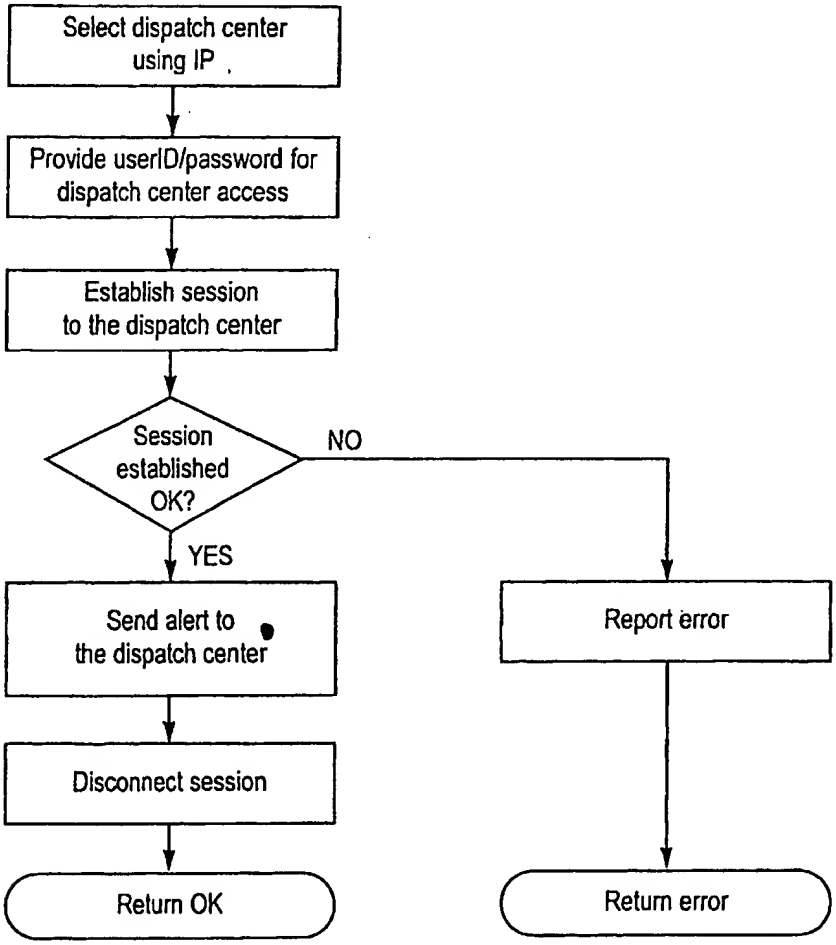


FIG. 10

Process to Obtain an IP Address from Secure Name Server 1 or Secure Name Server 2 for Customer Site

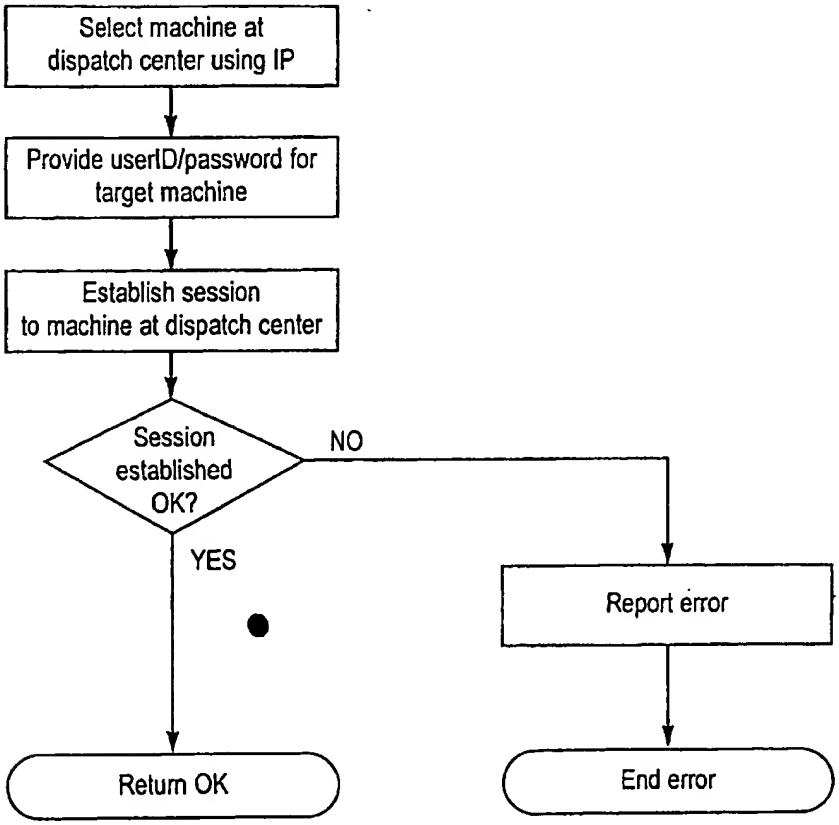


Process to Report an Alert to a Dispatch Center FIG. 11

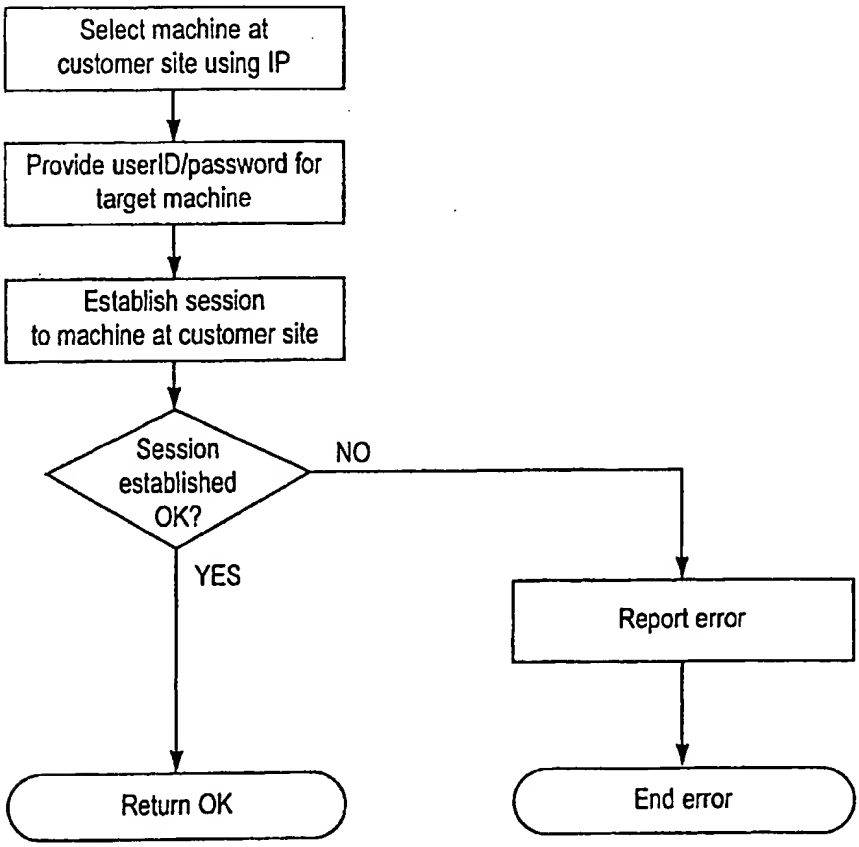


Connection Process to Dispatch Center Machine

FIG. 12



Connection Process to Customer Site Machine FIG. 13



COMBINED REMOTE ACCESS AND SECURITY SYSTEM

This is a continuation-in-part of U.S. patent application Ser. No. 08/752,249, filed Nov. 19, 1996, and entitled COMBINED REMOTE ACCESS AND SECURITY SYSTEM.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system that will provide remote access to allow servicing of a mainframe computer site while at the same time providing for security and integrity of the mainframe computer installation. In particular, the present invention is directed to a system wherein service and maintenance of the mainframe computer system is controlled and monitored from a remote location and service on the mainframe computer system may be performed by a remote support person at a further remote location.

2. Prior Art

Current mainframe processing environments use an operator console to display messages about the system. These messages are monitored and any problems are noted. Programmers and other technicians may then become involved in solving a problem. The problem may be beyond the operations staff's ability to handle.

The mainframe computer system may be serviced and monitored from a remote location. Remote support of mainframe computer installations is becoming increasingly important. This includes both remote monitoring and service support of mainframe computer systems. Businesses have been established which are capable of monitoring and maintaining a wide variety of mainframe computer installations.

From time to time, when problems are found, it is necessary for a technician, field engineer, or remote support person to have access to the mainframe computer system. A technician or field engineer can work on the problems on site at the mainframe installation. With high speed, broad band communications, it is possible for a remote support person or field engineer to diagnose and solve mainframe computer problems from a remote location by communication from a personal computer. Accordingly, the remote support person or field engineer may be at any location. These technicians are increasingly specialized and require wide access to the mainframe computer installation.

Moreover, it is increasingly a trend for employees, including those at mainframe computer installations, to work from their homes on personal computers. In this case, the employees' home computers must be connected to the mainframe computer installations.

At the same time, the computer mainframe installation must retain its security and integrity. In the past, while limited access and "firewalls" have sometimes been employed to maintain security, the field engineer or remote support person needs wide access to the mainframe computer to diagnosis and solve the problems.

Typically, the dispatch control center is located in a secure location. This dispatch control center may be at the same physical premises as the mainframe customer site or may be at a separate location remote from the mainframe. The remote support person, however, is often times at an unsecured location and may operate from a laptop or other unsecured central processing unit machine. Additionally, the mainframe computer business has only limited controls over the field engineer. For example, a disgruntled remote support person or field engineer with wide access to the mainframe computer system could cause considerable problems.

With both the dispatch control center and the support person at remote locations from the mainframe computer center, the channels of communication are important. While secure transmission lines are possible to establish, these are expensive over long distances. Additionally, the support person may be mobile.

The development of personal computers, modems (modulator/demodulator devices) and data connections has allowed the growth of many types of computer networks. The Internet, a somewhat public network of networks, has become an increasingly useful pathway for computer communication. There is, however, a concern about the security and integrity of the Internet pathways.

One solution to security on the Internet has been the encryption of data to be transmitted. One type of encryption uses a single "key" which the sender and recipient must keep secret. Another type of popular encryption uses "public-private keys." The first is a public key made available to anyone. The second is a "secret key" which the user must not allow anyone else to see. The public and private keys work in tandem. If the secret key is stored on a computer system, it is, however, vulnerable.

The same security issues and concerns may also exist on corporate intranets and private networks.

Accordingly, the present invention is directed to an arrangement where a mainframe or mainframes are secured at a customer site and wired to a personal computer with software for console monitoring. The console monitor is in communication with a secure dispatch control center location. The dispatch control center, upon being alerted of a problem, will contact a support person to diagnose and solve the particular problem. A data encryption key is randomly generated and transmitted from the dispatch control center to both the support person's central processing unit and to the console monitor of the mainframe.

It is a further object and purpose of the present invention to provide a remote access and security system using data encryption keys wherein a data encryption key is never transmitted or sent between the remote support person's central processing unit and the mainframe installation.

SUMMARY OF THE INVENTION

In a combined remote access and security system of the present invention, a single mainframe or multiple mainframes are located at a secure location. The mainframe or mainframes are connected to a console monitor central processing unit through a coax or twinax connection.

The console is used to display status messages about the mainframe computer system including errors or critical situations occurring on the computer system. When specified mainframe system alerts or problems occur a warning or alert will be issued. This alert will be communicated from the console to a dispatch control center central processing unit at a remote, secure location.

A dispatcher will monitor any alarm codes received from the mainframe system. The dispatcher will create a trouble ticket for each incoming alarm, assign a field engineer to the problem and call or otherwise contact the field engineer.

Thereafter, the dispatcher will initiate through the dispatch central processing unit, a unique, randomly generated user identification/password pair which is referenced to the assigned problem number. The user identification/password

pair is a data encryption key randomly generated by the dispatch central processing unit. The data encryption key is generated from a mathematical algorithm and will be a randomly generated binary code.

The identification/password encryption key is transmitted in two separate transmissions over two separate paths. The data encryption key is communicated from the dispatcher's central processing unit to the field engineer's central processing unit. Additionally, the dispatch central processing unit will also transmit the data encryption key back to the console central processing unit of the mainframe.

Once the field engineer has been notified and has received the identification/password pair from the dispatch control center, the field engineer will log on and communicate with the console central processing unit.

Data communicated from the field engineer's central processing unit to the console central processing unit is encrypted with the identification/password key. The data is subsequently decrypted upon receipt at the console monitor central processing unit. Importantly, the password/identification pair does not travel over the connection between the field engineer and the mainframe site.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a simplified schematic view of a combined remote access and security system as set forth in the present invention.

FIG. 2 illustrates a schematic view of an alternate embodiment of a combined remote access and security system as set forth in the present invention;

FIGS. 3A, 3B, 4, 5A, 5B and 6 are flow charts illustrating the sequential steps of the present invention; and

FIGS. 7 through 13 illustrate sub processes of those in FIGS. 3 through 6.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to the drawings in detail, FIG. 1 illustrates one preferred embodiment of a schematic diagram of a combined remote access and security system 10 of the present invention.

At a mainframe computer installation, a single mainframe 12 or multiple mainframes are located at a secure location (illustrated by the box 14). In many industries and businesses, large numbers of transactions are processed on an around-the-clock basis. Because of this demand, multiple mainframe central processing units are utilized within a secure computer complex. Access may be limited by physical measures, such as locked rooms, finger printing, and the like.

The mainframe or mainframes are connected to a console monitor central processing unit 16 which typically includes a keyboard 18 and display 20. The console 16 can be connected with the mainframe or mainframes in various ways, such as, by a coax or twinax connections 22.

The console 16, in the present situation, may employ a Windows NT™ operating system or other known operating systems. The operating system will have an application program or programs which is in a client-server format and provides console monitoring and console automation features. The application program watches or monitors the console for certain conditions.

The console 16 is used to display status messages about the mainframe computer system and allows the operations staff to control the operations of the mainframe or mainframes. Types of messages displayed may be about errors or critical situations occurring on the computer system. Examples of problems noted may be a tape drive fault or a fault in a chip on a board.

In today's environment, a single console may be responsible for multiple mainframe computers running multiple computer operating systems.

In specified mainframe system alerts, events or problems, the console will issue a warning or alert. This alert will be communicated from the console 16 through a modem and through a communications path, shown by arrow 30, to a dispatch control center, indicated by box 32. In the present embodiment, the communications path may be across the public Internet network. Each computer or machine will have a distinct Internet protocol address. Other communications paths, such as corporate intranets or private networks, are possible within the teachings of the present invention.

In the present embodiment, the secure dispatch control center 32 is located remote from the mainframe site, although the teachings of the invention apply if the dispatch center is at the same location.

The dispatch control center 32 is ordinarily at a secure location. Thus, access to the computer is limited by physical measures such as locked rooms, fingerprinting and the like. Additionally, access to the dispatch central processing unit 34 may require passwords prior to log on procedures. Typically, the dispatch central processing unit 34 includes a keyboard 36 and a display 38. The dispatch central processing unit 34 will be running a client side version of the application program running on the console monitor 16, as previously discussed.

A dispatcher (not shown) will monitor incoming alarm codes received from the mainframe 12. If an alert occurs, it will appear on the display screen 38 of the dispatcher. Upon receipt of an alarm code, it will display in a list on the display screen 38.

The dispatcher will create a trouble ticket for each incoming alarm in the problem tracking program. Alternatively, the procedure to create a problem or trouble ticket might be automated.

Once this has been completed, a field engineer or other remote support person will be assigned to the problem and will be called or otherwise contacted. In one such procedure, the dispatcher will call the field engineer or remote support person via telephone over a voice line. This connection is shown by arrow 40. The field engineer will be assigned a problem number for the incoming problem on the mainframe computer.

Thereafter, the dispatch control center will initiate a utility software program on the dispatch central processing unit 34 which will create a unique, randomly generated user identification/password pair which is referenced to the assigned problem number. In the FIG. 1 embodiments, the user identification/password pair is a data encryption key randomly generated by the dispatch central processing unit 34.

In the present case, the data encryption key is generated from a mathematical algorithm and will be a randomly generated binary code of 128 bits. The data encryption key is also time limited so that after a certain period of time, it will automatically expire. For example, the data encryption key may be valid for a period of 24 hours, after which it is no longer valid.

The identification/password pair is transmitted in two separate transmissions in two separate paths. The data

encryption key is communicated and transmitted from the dispatch central processing unit to a remote support person or field engineer central processing unit **50** as shown by arrow **52**. The field engineer central processing unit may take many forms, such as a laptop terminal, hand held PC or a desktop computer.

The dispatch central processing unit will also transmit the identification/password data encryption key back to the console central processing unit **16** as shown by arrow **24**. The data encryption key is itself also encrypted. The data encryption key is itself decrypted at the field engineer's central processing unit and at the console.

Once the field engineer or remote support person has been notified and has received the identification/password pair from the dispatch control center, the field engineer **50** will log on and communicate with the console central processing unit **16** as shown at arrow **54**. The field engineer will be running a client side version of the same application program.

The communication between the field engineer and the console may be made through a public network such as the Internet. The encrypted data is decrypted at the console monitor.

The field engineer or remote support person will input and download the assigned problem number already received from the dispatch control center **32**. The field engineer will thereby retrieve the problem details from the console. The field engineer will, thus, be connected to the mainframe site. Importantly, the password does not travel over the connection between the field engineer central processing unit **50** and the mainframe site **14**.

Once connected to the mainframe computer site, the field engineer or remote support person retrieves necessary information through the console central processing unit **16** via the coax **22** connection to the mainframe **12**. The field engineer, thus, has access to the mainframe and will endeavor to solve the problem presented.

Once the problem is resolved, the field engineer will notify the dispatch control center **32** that the problem has been resolved as shown at arrow **26**. This may be done in a number of ways. This may be done by telephone through voice line. Alternatively, the field engineer may communicate through the field engineer's central processing unit **50** through a communications line back to the dispatch central processing unit. This may also be performed through the Internet.

The dispatcher closes the problem in the problem tracking system. Thereafter, the unique identification/password pair is invalidated so that there is no longer access to the mainframe computer. The dispatcher closes the problem in the dispatch central processing unit database, which then removes the identification/password pair from the console monitor **16** at the mainframe site.

Each of the computer communications may be made through a public network such as the Internet. The data connection from an unsecured terminal/location is at all times secured by the present invention.

FIG. **2** illustrates an alternate embodiment **60** wherein the Internet protocol address are provided dynamically from a secure name server central processing unit.

At a mainframe computer installation, a single mainframe **62** or multiple mainframes will be located at a secure location (illustrated by box **64**). The mainframe or mainframes are connected to a console monitor central processing unit **66** which typically includes a keyboard **68** and a display **70**. The console **66** can be connected with the mainframe or mainframes in various ways, such as by coax or twinax connections **72**.

Alerts, events or problems will be noted by the console which will issue a warning or alert. This alert will be communicated from the console **66** through a modem and through a communications path, shown by arrow **74**, to a dispatch control center **76**. The dispatch control center includes a dispatch central processing unit **78** having a keyboard **80** and a display **82**. The dispatch central processing unit **78** will be running a client side version of the application program running on the console monitor. If an alert occurs at the console monitor, it will be transmitted and appear on the screen of the dispatch central processing unit. Upon receipt of an alarm code, it will display in a list on the display screen **82**. The dispatcher will create a trouble ticket for each incoming alarm in the problem tracking program. Alternatively, the procedure to create a problem or trouble ticket might be automated.

A field engineer or other remote support person will be assigned to the problem and will be called by a telephone or otherwise contacted which is shown by arrow **84**. Thereafter, the dispatch control central processing unit **72** will communicate with a secure name server **86** or **88**. The secure name server may be located on the premises of the dispatch control center or may be remote therefrom. The secure name server will, through a utility software program, generate a unique, randomly generated user identification/password pair. This will be referenced to the assigned problem number. The user identification/password pair is a data encryption key randomly generated. The data encryption key is transmitted in two separate transmissions over two separate paths. The data encryption key is communicated and transmitted from the dispatch central processing unit **78** to a remote support person or field engineer central processing unit **90** as shown by arrow **92**.

The dispatch central processing unit will also transmit the data encryption key back to the console central processing unit **68** which is shown by arrow **94**.

After the field engineer or support person has been notified and has received the identification/password pair from the dispatch control center, the field engineer will log on and communicate with the console processing unit **68** as shown by arrow **96**.

Once the problem has been resolved, the field engineer or support person will notify the dispatch control center that the problem has been resolved. This is illustrated by arrow **98**. The dispatcher at the dispatch control center closes the problem in the problem tracking system. Thereafter, the unique identification/password pair is invalidated so that there is no longer access to the mainframe computer site **64**. The dispatcher closes the problem in the dispatch central processing unit database which then removes the identification/password pair from the console monitor **68** at the mainframe site.

FIGS. **3** through **13** illustrate the process of the present invention that will provide remote access to allow servicing of the mainframe computer while providing for security and integrity of the mainframe computer installation. The process will be described in relation to the FIG. **2** embodiment with a pair of dispatch control centers. FIGS. **3A** and **3B** illustrate the initial process at the secure customer mainframe site **14** to monitor for alerts. After the process has been started, as shown at **100**, the console will be checked for alert situations illustrated at box **102**.

If there is no unreported alert, as at **104**, a check will be made to see whether the reporting interval has expired **106**.

If the reporting period has expired **106**, then the current Internet protocol address (IP) will be registered with a first secure name server, as seen at **108**. If the first secure name server does not register the Internet protocol address, then the current Internet protocol address will be registered with the second secure name server as seen at **110**.

Returning to box **104**, if there is an unreported alert, an Internet protocol address will be obtained for the first dispatch control center from a secure name server central processing unit as shown at **112**. The secure name server is a repository of customer sites and their current IP addresses. Once the Internet protocol address has been obtained for dispatch center **1**, an alert will be reported to the first dispatch center, as seen at **116**.

If the report on the alert has been received, box **118**, then the process can continue. If there is no success, then, as shown on FIG. **3B**, an Internet protocol address will be obtained for dispatch center **2** from either secure name server, as shown at **120**. If an internal protocol address has been obtained for the second dispatch center as shown at **122**, the alert will be reported to the second dispatch center as shown at box **124**. If the alert is reported as shown at **126**, the process will again continue in same manner.

FIG. **4** illustrates the process for a dispatch control center to handle an incoming alert from a secure mainframe customer site. The FIG. **4** process would chronologically follow the process described in FIGS. **3A** and **3B**. The dispatch control center will receive an alert from the mainframe customer site **130**. A problem ticket or problem number will be created in a tracking system as shown at box **132**. A unique user ID/password pair for the remote support person will be generated, as at box **134**. An Internet protocol address for the customer site will be obtained from a secure name server, as seen in box **136**. Obtaining an IP address for the customer site will be explained in detail below.

Once the Internet protocol address has been obtained for the customer site as shown at **138**, a connection will be made from the dispatch control center to the customer site as shown at **140**.

The remote support person's user ID/password pair will be set up on the customer mainframe site **142**. After the connection with the customer site has been disconnected **144**, a remote support person will be selected from an availability list **146**. The remote support person may be contacted in various fashions, such as by telephone, and given the problem number **148**.

FIG. **5** illustrates the process for the remote support person or field engineer that would be employed to handle the problem that has been reported. This procedure would chronologically follow the process shown in FIG. **4**.

As seen in FIG. **5A**, once a problem has been received from the dispatch control center as shown at box **152**, an Internet protocol address for the dispatch control center will be obtained from one of the secure name servers **154**. This process will be explained in detail below.

Once the Internet protocol address has been obtained for the dispatch control center as shown at **156**, a connection will be made to the dispatch center **158**. The name and details for the secure mainframe customer site will be provided **160**. Thereafter, the remote support person will disconnect from the dispatch control center **162**.

An Internet protocol address will be obtained for the customer site from either of the secure name servers **164**. Once the Internet protocol address for the mainframe customer site has been obtained **166**, the remote support person will connect to the customer site using the Internet protocol as shown at **170**. The remote support person or field engineer will be able to work to solve the particular problem as seen at box **172** and, thereafter, disconnect from the mainframe customer site **174**.

An Internet protocol address will be obtained for the dispatch control center from either secure name server as shown at **176**.

Once the Internet protocol address has been obtained by the support person for the dispatch center **178**, the remote support person will connect to the dispatch control center using that Internet protocol address **180**. The support person will be able to report completion of the assignment and closing of the problem record **182**. The support person will thereafter disconnect from the dispatch center, as shown at **184**.

FIG. **6** illustrates the next sequential process in the overall system of the present invention. The dispatch control center will invalidate the remote support person's user ID/password at the secure mainframe customer site.

The dispatch control center will obtain an Internet protocol address for the mainframe customer site from either secure name server, as shown at **190**. Once an Internet protocol address has been obtained **192**, a connection will be made between the dispatch control center to the console monitor at the customer site using the Internet protocol address as shown at **194**. If no Internet protocol address has been obtained, an error will be reported as shown at box **188**.

The dispatch center's unique user ID/password will be provided to the console at the customer site, as seen at box **196**. A session will thereby be established to the console monitor at the mainframe customer site (**198**). The remote support person's user ID/password on the customer site console will be invalidated as shown at step **200**, following which the session will be disconnected **202**.

The remaining processes illustrated in FIGS. **7** through **13** are sub-processes of the foregoing.

FIG. **7** illustrates the process to register a computer with a secure name server central processing unit. A target secure name server will be selected by its Internet protocol address, as shown at box **210**. The secure name server will be provided an access user ID/password pair as seen at box **212**. A session will thereby be established to the server as shown at **214**. If the session has been established **216**, the Internet protocol address for the named machine will be registered **218**. This process is also seen in FIG. **3A** at boxes **108** and **110**.

FIG. **8** illustrates the process to obtain an Internet protocol address from a secure name server. This process is shown at box **112** in FIG. **3A**. As seen in FIG. **8**, a secure name server will be selected by its Internet protocol address, as seen at box **220**. The secure name server will be provided with an access user ID/password **222** in order to establish a session **224**. Once a session has been established, as shown at **226**, an Internet protocol address will be requested for the console monitor **228**. If the named computer has been defined **230**, a check will be made whether the named machine has its address registered **232**, and if the registration is up-to-date **234**.

FIG. **9** illustrates the process for either of two secure name servers to obtain an IP address initially from one server and, if not successful, from a second server. This process would be utilized at **176** in FIG. **5B**.

FIG. **10** illustrates a process to obtain Internet protocol address for a mainframe customer site from initially a first server and, thereafter, a second server for the customer mainframe site.

FIG. 11 illustrates the subprocess to report an alert from the mainframe customer site to a dispatch center. This step is illustrated in FIG. 3A at box 116.

The subprocess to connect a remote support person or field engineer to a dispatch center is illustrated in FIG. 12.

Finally, the subprocess to connect to the console at a mainframe customer site using the Internet protocol address is illustrated in FIG. 13.

Whereas, the present invention has been described in relation to the drawings attached hereto, it should be understood that other and further modifications, apart from those shown or suggested herein, may be made within the spirit and scope of this invention.

What is claimed is:

1. A combined remote access and security system for servicing a secure mainframe central processing unit having a console monitor, which system comprises:

a secure dispatch control central processing unit for receiving problem reports concerning said mainframe central processing unit;

communications means for communicating between said mainframe from said console monitor and said dispatch control central processing unit;

a field engineer central processing unit independent from said secure mainframe central processing unit and said secure dispatch control central processing unit, wherein said secure dispatch control central processing unit is remote from said mainframe central processing unit and wherein said field engineer central processing unit is remote from both said mainframe central processing unit and said dispatch control central processing unit;

communication means for communicating between said field engineer central processing unit and said dispatch control central processing unit;

a data encryption key randomly generated and transmitted from said dispatch control central processing unit on separate paths and in separate transmissions to both said field engineer central processing unit and said mainframe central processing unit; and

communication means between said field engineer central processing unit and said mainframe central processing unit wherein all data transmitted from said field engineer central processing unit is encrypted and wherein said encrypted data received is decrypted at said mainframe central processing unit.

2. A combined remote access and security system as set forth in claim 1 wherein said data encryption key is time limited to expire after a set time period.

3. A combined remote access and security system as set forth in claim 1 wherein said communications means between said mainframe central processing unit and said dispatch central processing unit, between said field engineer central processing unit and said dispatch central processing unit and between said field engineer central processing unit and said mainframe central processing unit is via the Internet network.

4. A combined remote access and security system as set forth in claim 1 wherein said console monitor includes a central processing unit having monitoring and automation capabilities.

5. A combined remote access and security system as set forth in claim 4 including a plurality of mainframe central processing units connected to said console.

6. A combined remote access and security system as set forth in claim 1 wherein said communications means for communicating between said mainframe and said dispatch control central processing unit and said communications means between said field engineer central processing unit and said dispatch control central processing unit are through a communications path with each said central processing unit has a distinct Internet protocol address.

7. A combined remote access and security system as set forth in claim 6 wherein said Internet protocol addresses are stored in a secure name server.

8. A process to remotely access and service a secure mainframe central processing unit having a console monitor, which process comprises:

communicating a problem with said mainframe central processing unit from said console monitor to a remote dispatch control center central processing unit;

randomly generating a data encryption key at said remote dispatch control center processing unit;

transmitting said data encryption key from said remote dispatch control center on separate paths in separate transmission to both said mainframe central processing unit and to a field engineer central processing unit, wherein said field engineer central processing unit is independent and remote from both said mainframe central processing unit and said dispatch control central processing unit; and

communicating between said field engineer central processing unit and said mainframe wherein all data transmitted from said field engineer central processing unit is encrypted and then decrypted at said mainframe central processing unit.

9. A process to remotely access and service a secure mainframe central processing unit as set forth in claim 8 including the additional step of time limiting the data encryption key to expire after a set period of time.

10. A process to remotely access and service a secure mainframe central processing unit as set forth in claim 8 including the additional, initial step of monitoring said console monitor for certain conditions which are identified as problems.

11. A process to remotely access and service a secure mainframe central processing unit as set forth in claim 8 wherein the steps of communicating said problem, transmitting said data encryption key, and communicating between said field engineer central processing unit and said mainframe are done over the Internet network.

12. A process to remotely access and service a mainframe central processing unit as set forth in claim 8 including the additional step of the dispatch control center contacting said field engineer after communicating said problem to said dispatch control center.

* * * * *

US006499108B1

(12) **United States Patent**
Johnson

(10) **Patent No.: US 6,499,108 B1**
(45) **Date of Patent: Dec. 24, 2002**

(54) **SECURE ELECTRONIC MAIL SYSTEM**

(76) Inventor: **R. Brent Johnson**, 111 W. 5th St., Suite 300, Tulsa, OK (US) 74103

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/239,425**

(22) Filed: **Jan. 28, 1999**

Related U.S. Application Data

(63) Continuation-in-part of application No. 08/892,982, filed on Jul. 15, 1997, now Pat. No. 5,970,149, which is a continuation-in-part of application No. 08/752,249, filed on Nov. 19, 1996, now abandoned.

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **713/201**; 713/184; 713/176; 380/28

(58) **Field of Search** 380/28; 713/201, 713/176, 184

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,182,933	A	1/1980	Rosenblum	179/1.5
4,310,720	A	1/1982	Check, Jr.	178/22.08
4,430,728	A	2/1984	Beitel et al.	364/900
4,531,023	A	7/1985	Levine	179/2
4,578,531	A	3/1986	Everhart et al.	178/22.08
4,763,351	A	8/1988	Lipscher et al.	379/95
4,965,804	A	10/1990	Trbovich et al.	380/21
5,179,695	A	1/1993	Derr et al.	395/575
5,204,961	A	4/1993	Barlow	395/725
5,237,677	A	8/1993	Hirosawa et al.	395/575
5,347,578	A	9/1994	Duxbury	380/4
5,416,842	A	5/1995	Aziz	380/30
5,452,460	A	9/1995	Distelberg et al.	395/700
5,537,554	A	7/1996	Motoyama	395/280
5,550,984	A	8/1996	Gelb	395/200
5,678,002	A	10/1997	Fawcett et al.	395/183
5,708,655	A *	1/1998	Toth et al.	370/313

FOREIGN PATENT DOCUMENTS

EP	0474058 A2		3/1992	G06F/11/00
FI	WO 99/03238	*	1/1999	H04L/12/58

OTHER PUBLICATIONS

Andrew Tanenbaum, Computer Networks, Prentice Hall, pp. 643–670.*

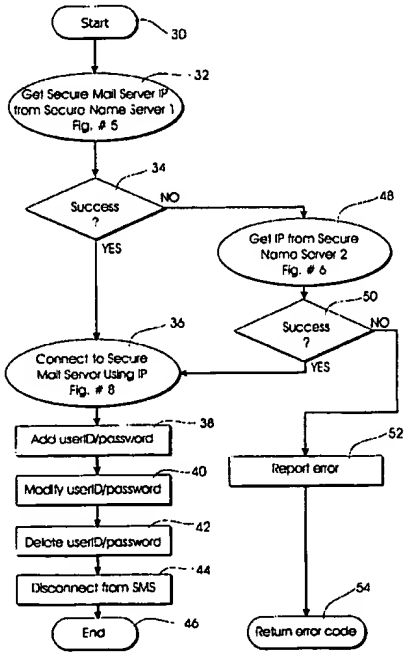
* cited by examiner

Primary Examiner—Gail Hayes
Assistant Examiner—James Seal
(74) *Attorney, Agent, or Firm*—Head, Johnson & Kachigian

(57) **ABSTRACT**

A system and method for transferring messages securely over a computer network which includes the steps of inputting the message to be transmitted at a first device and then encrypting the message at the first device. An address for a dynamically-addressed server is obtained and the first device is connected to the dynamically addressed server. The encrypted message is transmitted from the first device to the server and the message is received at the dynamically addressed server. The message is transmitted from the server to a second device and then the message is decrypted at the second device.

11 Claims, 8 Drawing Sheets



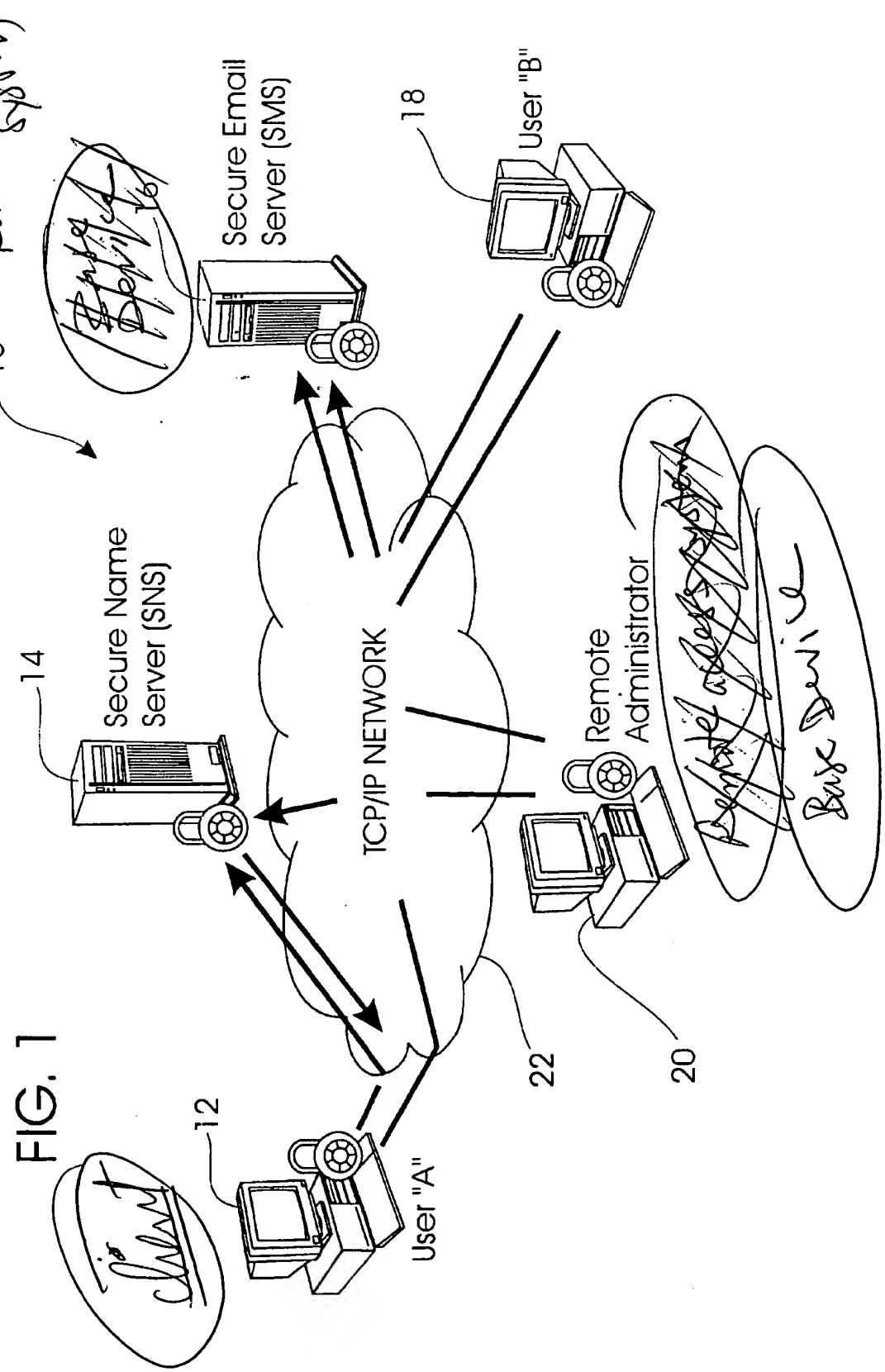

10
Secure Email Server (SMS)
18
User "B"
Secure Name Server (SNS)
14
TCP/IP NETWORK
Remote Administrator
22
20
12
User "A"

FIG. 1

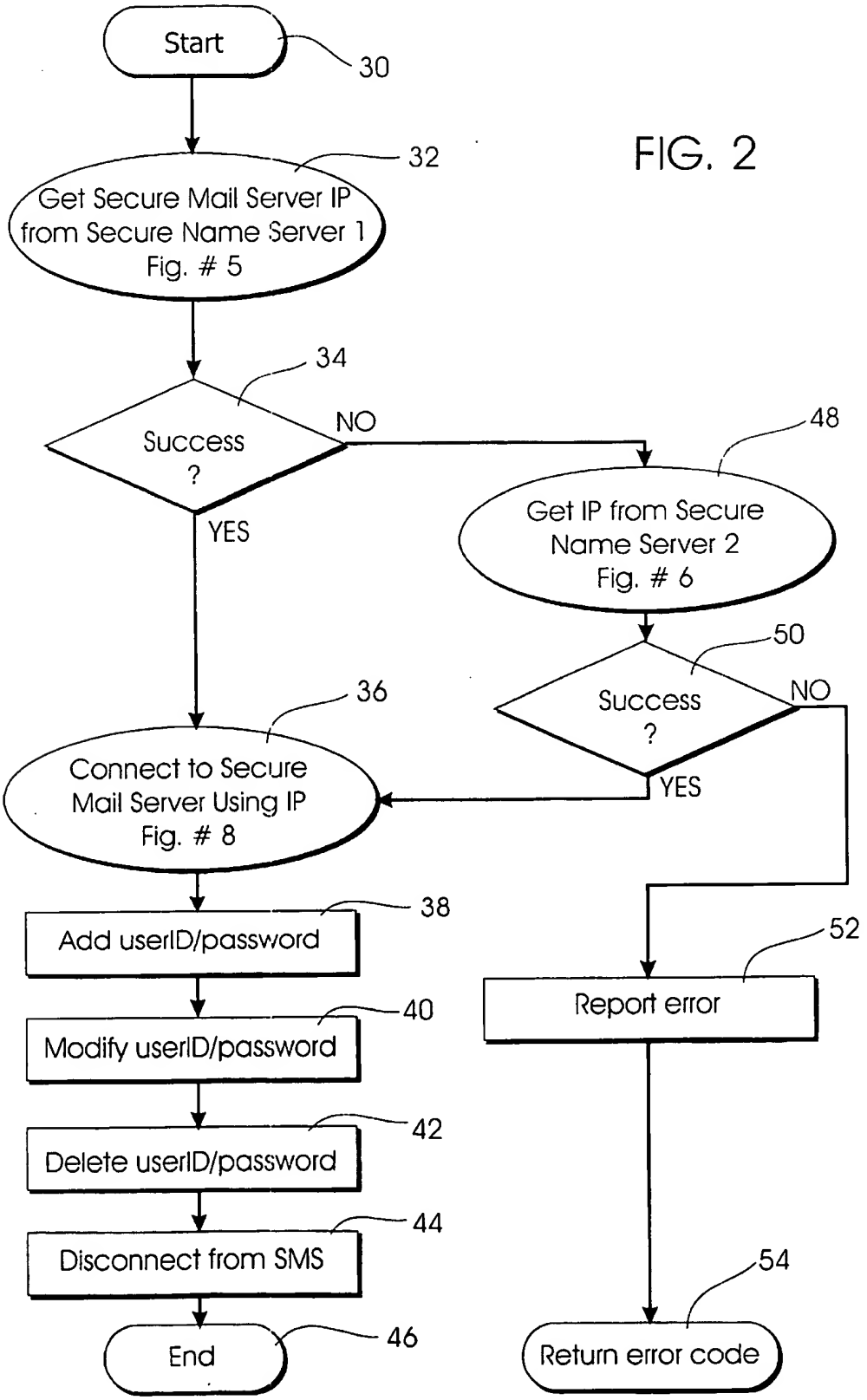

Start
30
Get Secure Mail Server IP from Secure Name Server 1 Fig. # 5
32
Success ?
34
NO
YES
Get IP from Secure Name Server 2 Fig. # 6
48
Success ?
50
NO
YES
Connect to Secure Mail Server Using IP Fig. # 8
36
Add userID/password
38
Modify userID/password
40
Delete userID/password
42
Disconnect from SMS
44
End
46
Report error
52
Return error code
54

FIG. 2

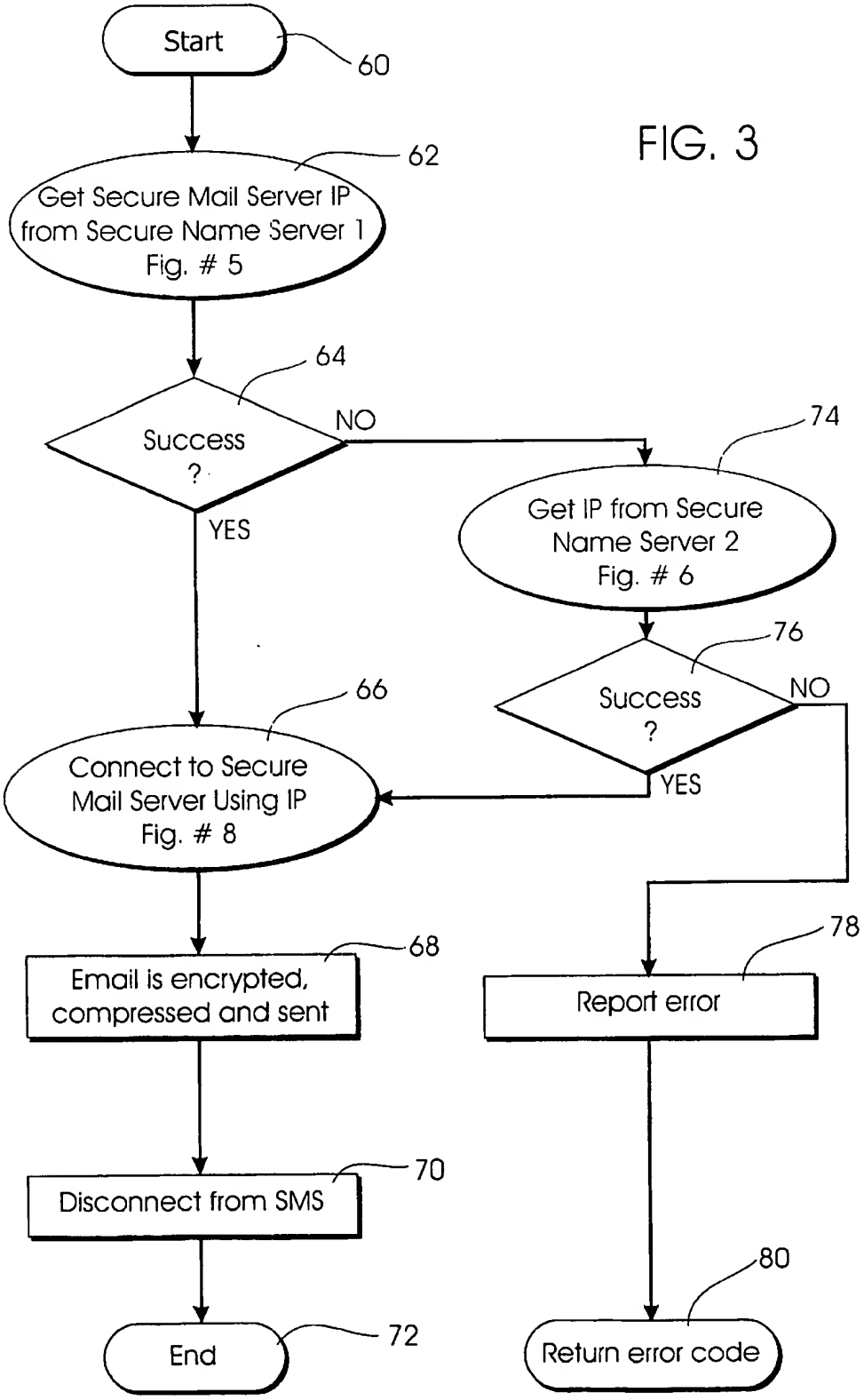

Start
60
Get Secure Mail Server IP from Secure Name Server 1 Fig. # 5
62
Success ?
64
NO
YES
Get IP from Secure Name Server 2 Fig. # 6
74
Success ?
76
NO
YES
Connect to Secure Mail Server Using IP Fig. # 8
66
Email is encrypted, compressed and sent
68
Report error
78
Disconnect from SMS
70
End
72
Return error code
80

FIG. 3

FIG. 4

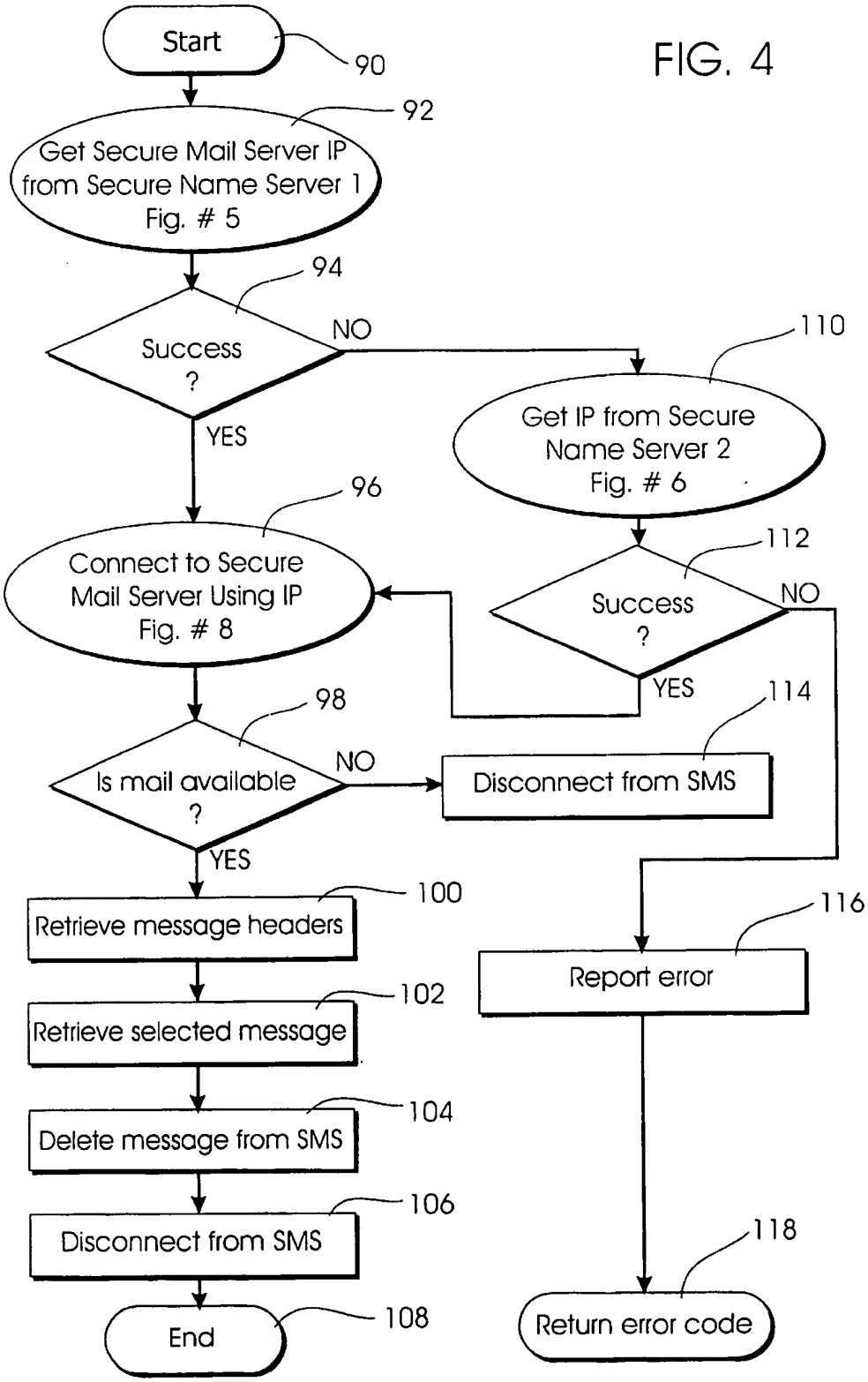

Start
90
92
Get Secure Mail Server IP from Secure Name Server 1 Fig. # 5
94
Success ?
NO
YES
110
Get IP from Secure Name Server 2 Fig. # 6
96
Connect to Secure Mail Server Using IP Fig. # 8
112
Success ?
NO
YES
98
Is mail available ?
NO
YES
114
Disconnect from SMS
100
Retrieve message headers
102
Retrieve selected message
104
Delete message from SMS
106
Disconnect from SMS
108
End
116
Report error
118
Return error code

FIG. 5

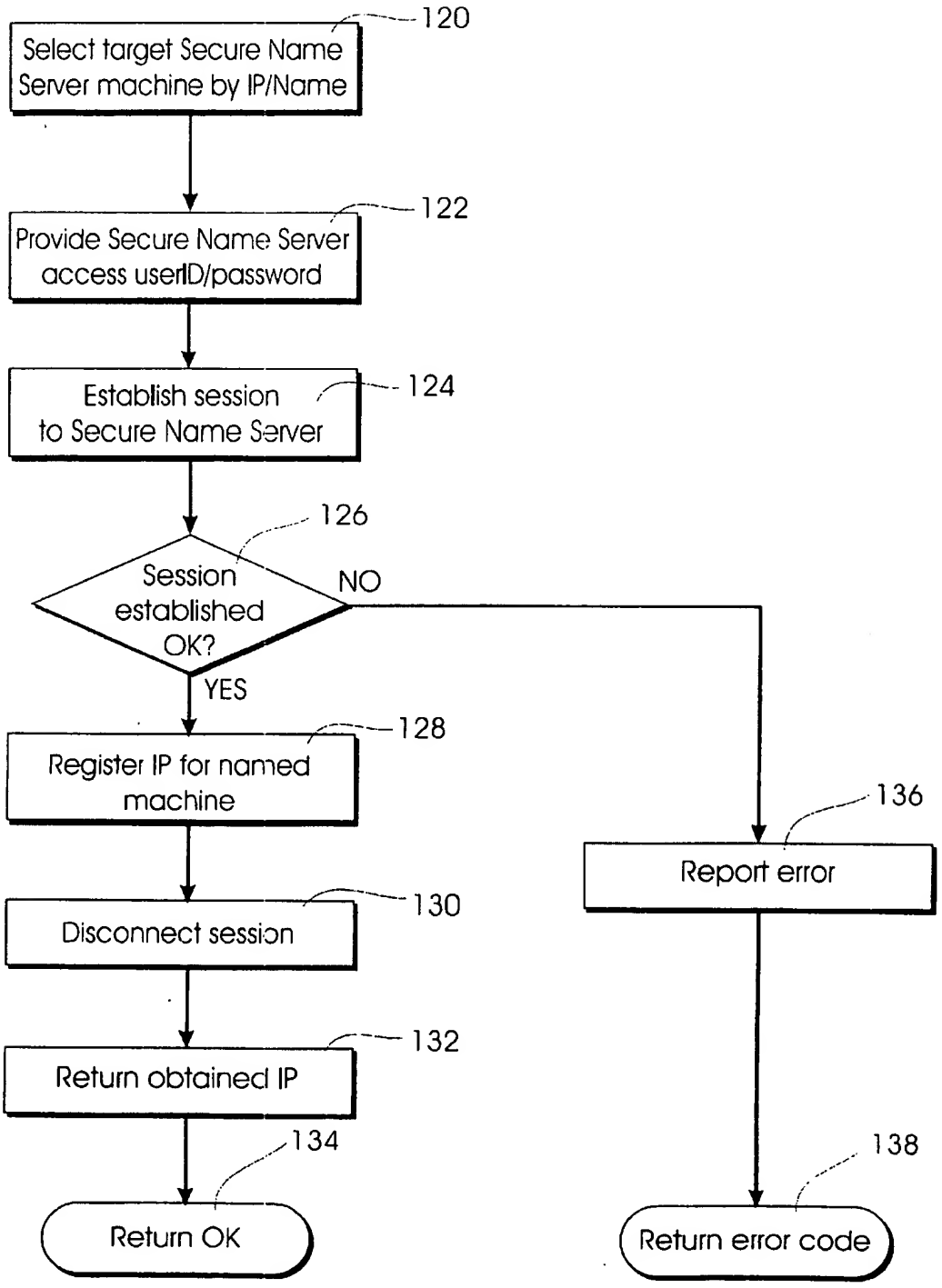
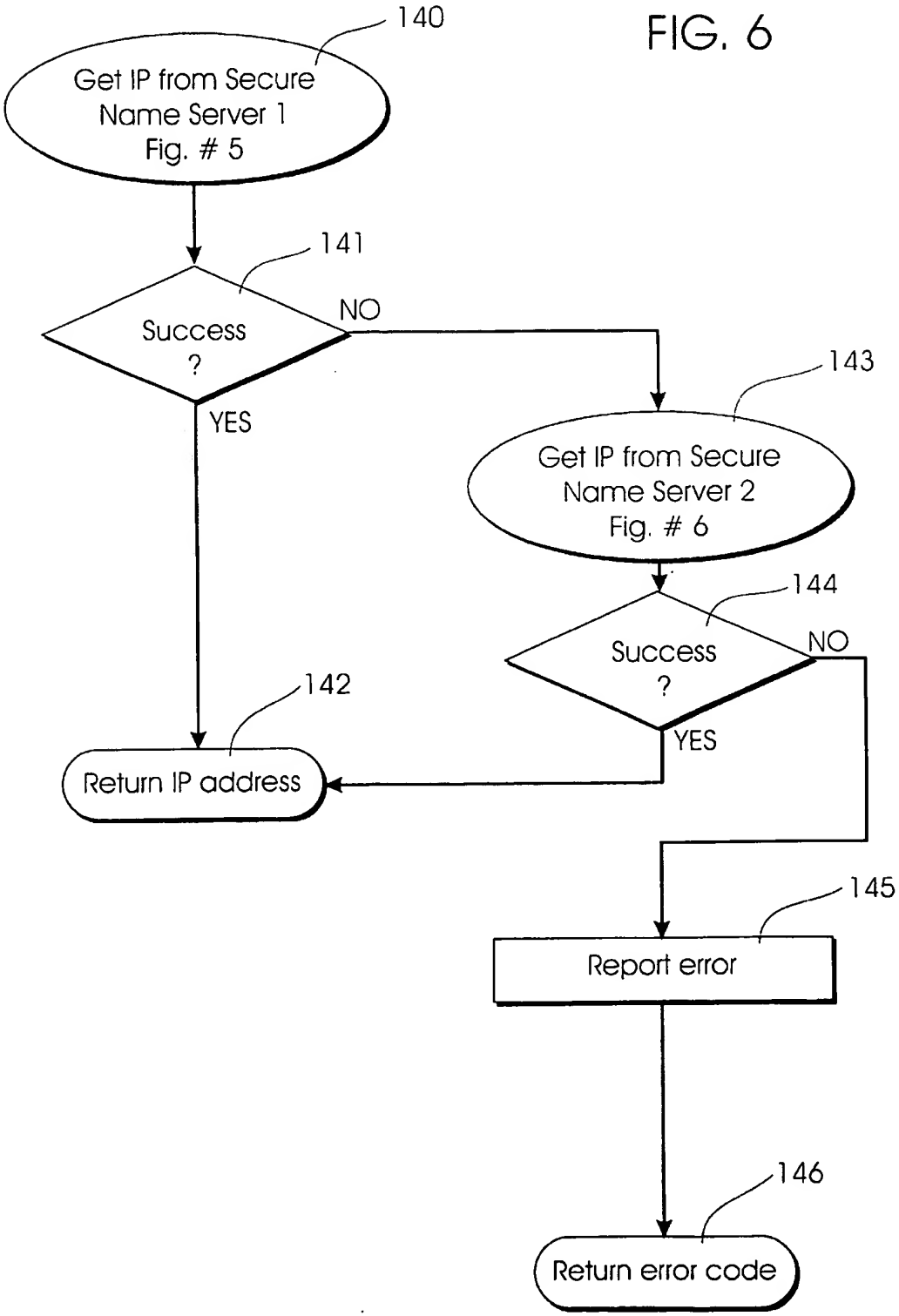

120
Select target Secure Name Server machine by IP/Name
122
Provide Secure Name Server access userID/password
124
Establish session to Secure Name Server
126
Session established OK?
NO
YES
128
Register IP for named machine
130
Disconnect session
132
Return obtained IP
134
Return OK
136
Report error
138
Return error code

FIG. 6


140
Get IP from Secure Name Server 1 Fig. # 5
141
Success ?
NO
YES
143
Get IP from Secure Name Server 2 Fig. # 6
144
Success ?
NO
YES
142
Return IP address
145
Report error
146
Return error code

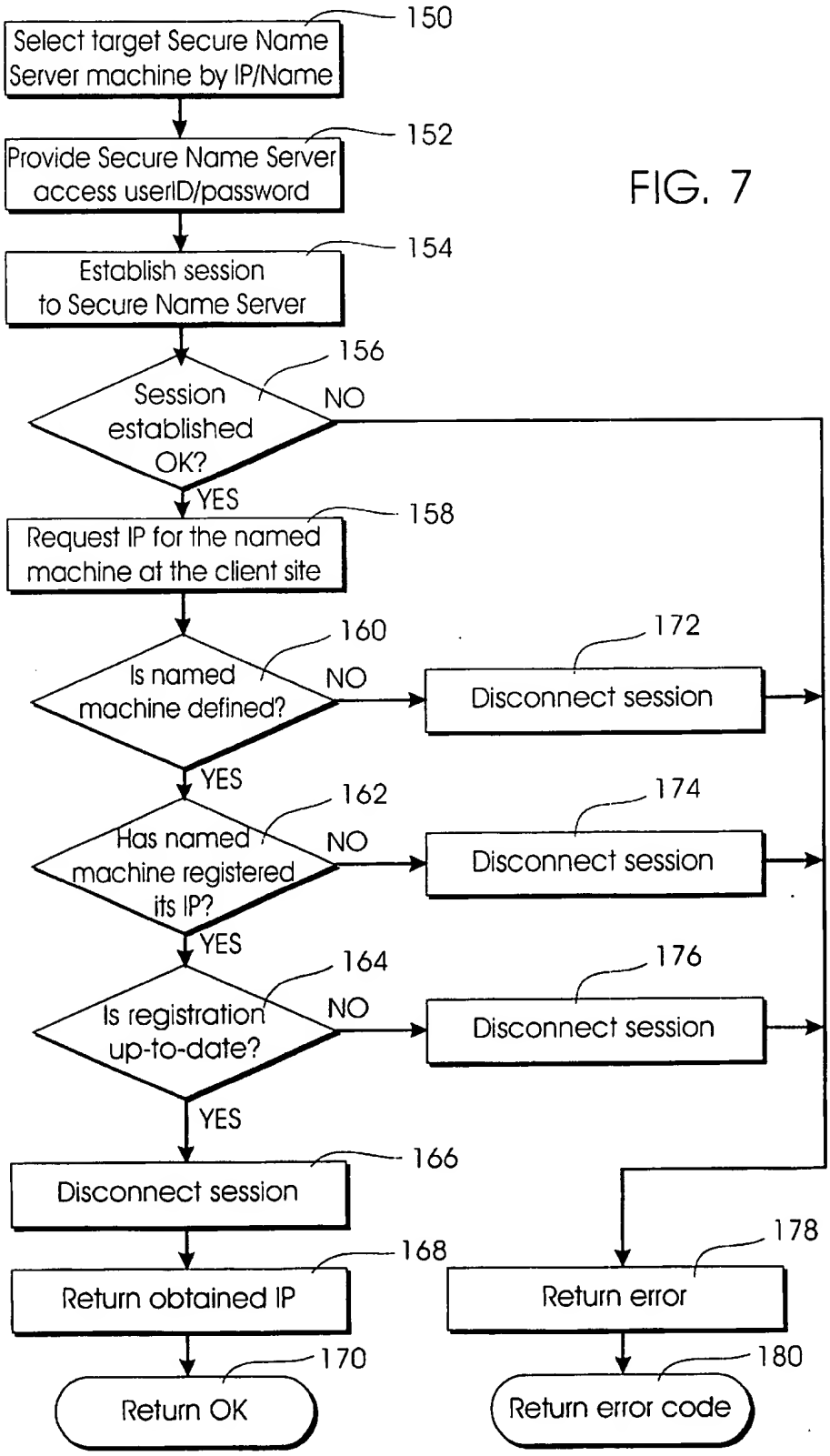
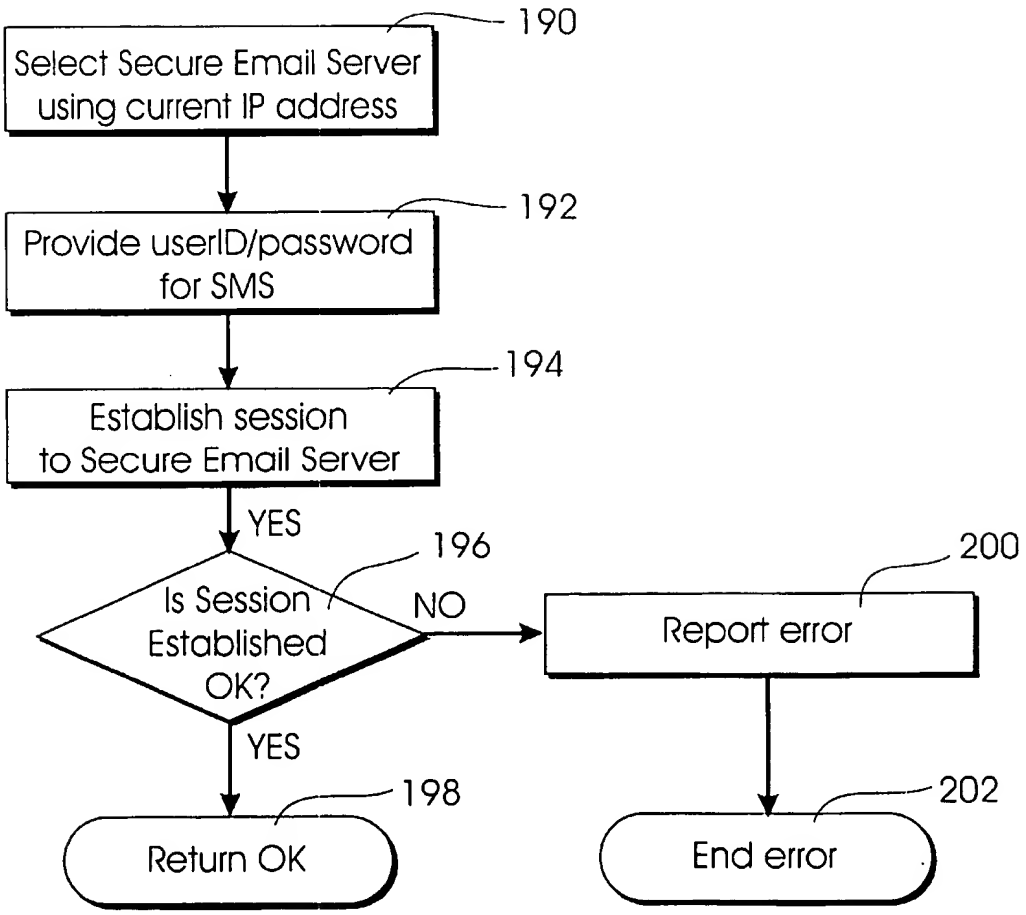

150
Select target Secure Name Server machine by IP/Name
152
Provide Secure Name Server access userID/password
154
Establish session to Secure Name Server
156
Session established OK?
NO
YES
158
Request IP for the named machine at the client site
160
Is named machine defined?
NO
172
Disconnect session
YES
162
Has named machine registered its IP?
NO
174
Disconnect session
YES
164
Is registration up-to-date?
NO
176
Disconnect session
YES
166
Disconnect session
168
Return obtained IP
178
Return error
170
Return OK
180
Return error code

FIG. 7

FIG. 8


190
Select Secure Email Server using current IP address
192
Provide userID/password for SMS
194
Establish session to Secure Email Server
YES
196
Is Session Established OK?
NO
200
Report error
YES
198
Return OK
202
End error

SECURE ELECTRONIC MAIL SYSTEM

REFERENCE TO APPLICATIONS

This application is a continuation-in-part of U.S. patent application Ser. No. 08/892,982 filed Jul. 15, 1997, now U.S. Pat. No. 5,970,149 and entitled "Combined Remote Access and Security System"; which is a continuation-in-part of U.S. patent application Ser. No. 08/752,249, filed Nov. 19, 1996, and entitled "Combined Remote Access and Security System" now abandonded.

REFERENCE TO MICROFICHE APPENDIX

This application is not referenced in any microfiche appendix.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is directed to an apparatus and method for a secure electronic mail communication system. More particularly, the invention is directed for use in communicating over networks where secure information exchange is required. The invention has utility in applications such as person-to-person communication over network systems, communications over the Internet, interbusiness network communications where security is required, and the like.

2. Prior Art

The use of keys for secure communications is well known. Secure communication systems, as well as key systems, are shown in U.S. Pat. No. 4,182,933, issued to Rosenblum on Jan. 8, 1980, entitled "Secure Communication System With Remote Key Setting"; U.S. Pat. No. 4,310,720, issued to Check, Jr. on Jan. 12, 1982; entitled "Computer Accessing System"; U.S. Pat. No. 4,578,531, issued to Everhart et al., on Mar. 25, 1986, entitled "Encryption System Key Distribution Method and Apparatus"; U.S. Pat. No. 4,965,804, issued to Trbovich et al. on Oct. 23, 1990, entitled "Key Management for Encrypted Packet-Based Networks"; U.S. Pat. No. 5,204,961, issued to Barlow on Apr. 20, 1993, entitled "Computer Network Operating With Multi-Level Hierarchial Security With Selectable Common Trust Realms and Corresponding Security Protocols"; and U.S. Pat. No. 5,416,842, issued to Aziz on May 16, 1995 entitled "Method and Apparatus For Key-Management Scheme For Use With Internet Protocols At Site Firewalls".

U.S. Pat. No. 4,182,933, issued to Rosenblum on Jan. 8, 1980, discusses a "Secure Communication System With Remote Key Setting". The Rosenblum '933 patent describes a system wherein a first subscriber communicates with a key distribution center to get an updated key to initiate secure communications with a second subscriber. An overview of the system shows that the user dials a telephone number into the first subscribing unit. The first subscribing unit then places the telephone number into temporary memory storage. The first subscriber then retrieves its initial caller variable from memory and places it into a key generator. The first subscriber then retrieves the number of the key distribution center (KDC) from its memory and dials the number. Once a connection has been established the first subscriber sends its caller ID as well as the caller ID of the telephone number being called to the KDC. This information is not yet transmitted in a secure manner.

Once the KDC has received the information from the first subscriber, the KDC looks up the caller variable for both the first subscriber and for the telephone number being called. The KDC then generates a new caller variable for the first telephone number. The KDC then transmits the caller variable for the number being called, a new caller variable for the first subscriber, using a secure transmission controlled by the initial caller variable. If this transmission is successful, then the KDC will replace the old caller variable in its table format with a new caller variable and break the connection.

Once the first subscriber has received and deciphered the caller variable for the number to be called and its new key caller variable, it will replace the old and used initial caller variable key with the new caller variable key. The first subscriber will then send the key for the number to be called to the key generator, retrieve the telephone number to be called, and dial the telephone number. The first subscriber will then transmit any information input by the user to the second subscriber using the second subscriber key. The second subscriber will receive information that has been encoded with the second subscriber key and will decode the information and transfer it on to the second user. In an alternative embodiment, after the phone call between the first subscriber and second subscriber, the second subscriber will call and get a new key from the KDC. In this alternative embodiment, both the key for the first subscriber and for the second subscriber will be changed out on every telephone call.

U.S. Pat. No. 4,310,720, issued to Check, Jr. on Jan. 12, 1982 discloses a "Computer Accessing System". The specification discloses a method for communicating between an access unit and a computer. The user enters his password into an input device which is connected to an access unit. The access unit generates a pseudo random access key from the password that is entered. The access unit then sends the access unit number and the generated access key to the computer controller for access to the computer system. The computer controller receives the access unit number and access key. The computer controller then verifies the access unit number. If the access unit number is properly verified, the computer controller will then compare the access code to the expected access code listed in a table in the computer's memory. This expected access code is generated using a congruent pseudo-random decoding algorthym. If the access key code and the expected code match, then the computer controller will establish a link between the access unit and the computer.

The access unit and the computer will talk through an encoded communication system. Both the access unit and the computer will use a randomly generated encryption key for encoding and decoding the communication. This key is independently generated by both the access unit and the computer and is not transmitted over the access unit to computer link. After the termination of the call between the access unit and the computer, the computer will generate and store the next access key number for that particular access unit.

U.S. Pat. No. 4,578,531 issued to Everhart et al. on Mar. 25, 1986 discloses an "Encryption System Key Distribution Method and Apparatus". This system allows the secure method for communication between a terminal "A" and terminal "B" by using a remote key distribution center. An initial signal is sent from terminal "A" to terminal "B" to initiate the process of generating a secure communication line. Terminal "A" then generates a new call set up key in preparation for communication with the key distribution center, and a partial session key which will be transmitted through the key distribution center to terminal "B". Terminal "A" then updates its verification information in preparation

for communication with the key distribution center. Terminal "A" then initiates the connection with the key distribution center to which it sends its terminal address and the terminal "B" address and an encrypted message including the two generated keys and the verification information. At this point, terminal "A" will wait for the processing by the key distribution center.

The key distribution center will read the address information from the signal sent from terminal "A" and use this to access a de-cryption key previously sent in communication with terminal "A". The message from terminal "A" will then be de-crypted and the verification information will be updated. The key distribution center will then generate a bidirectional asymmetric encryption/de-cryption key pair. The first part of this key pair will be sent to terminal "A", and the second part of the key pair will be sent to terminal "B". A similar communication will happen with terminal "B".

The message to terminal "A" will consist of a subsequent call key for the next communication with a KDC, a partial session key which it received from terminal "B", verification information, and two other variables "Y" and "Q". These five pieces of information will be encrypted using the call set up key for the present communication with terminal "A" and the information will be transmitted to terminal "A". A similar encrypted message will also be sent to terminal "B" from the KDC.

Terminal "A" will de-crypt the message from the KDC and verify that the information is correct. Terminal "A" will then store the new communication key for the next communication with the KDC, take down the channel to the KDC, and establish a communication channel with terminal "B". A similar process will happen at terminal "B". At this point, terminal "A" and "B" will be able to communicate securely using the partial keys that were exchanged through the KDC. Terminals "A" and "B" can then use a random number and the variables "Y" and "Q" to create a new key which may be used to communicate securely between terminals "A" and "B". By using the variables and a random number to generate a new communication key, a secure communication encryption message may be employed which cannot be known by any outsiders to terminal "A" and "B", including the KDC.

U.S. Pat. No. 4,965,804, issued to Trbovich et al., on Oct. 23, 1990, discloses a "Key Management For Encrypted Packet Based Networks". This method of key management uses a key distribution center for sending keys to remote locations so that a secure communication can be made. Specifically, the system is designed to be compatible with X.25 type packet switching networks. This compatibility requires a balanced transmission which is implemented by a transparent device between the source DTE and second YDTE. The source DTE sends a transmit request to the transparent device which responds with a dummy signal back to the source DTE. The transparent device then contacts the key management system and obtains a key. A similar key is sent to the transparent device for the second DTE. The transparent devices for the first DTE and the second DTE then establish a communication network with an encrypted signal transfer, and finally the source DTE talks to the second DTE through the transparent devices and the encrypted connection.

U.S. Pat. No. 5,204,961, issued to Barlow on Apr. 20, 1993, discloses a "Computer Network Rating With Multi-Level Hierarchial Security With Selectable Common Trust Realms and Corresponding Security Protocols". The invention involves a method for setting up network communications between two trusted computer systems. Each trusted computer has a common set of protocols for the protection of data contained therein. Thus, if a user for a trusted computer system attempts to send data to a non-trusted computer system, then the trusted computer system will stop the message transfer and will not allow the communication to occur. This system operates as a method for two trusted computers to talk over a network which is not physically secure against interlopers. Each computer that is a member of a specific trust realm enforces a predefined security policy and defines security levels for the data contained within the computer. Before a trusted computer transmits a specified message, the trusted computer checks the trust realm table to verify that both the transmitting and receiving computers are part of at least one common trust realm. If both computers are part of a common trust realm, then the message will be transferred using the appropriate protocol for that trust realm. If the computers are not both members of the trust realm, then the message will not be transmitted. The communication between two trusted computers consists of a message which is transmitted as a protocol data unit which includes a sealed version of the message, authenticated identifies for the sending system and user, the message security level label, and an identifier for the selected trust realm. The transmitted message is then received, processed for validity and if valid, the message is processed within the receiving computer.

U.S. Pat. No. 5,416,842, issued to Aziz on May 16, 1995, discloses a "Method and Apparatus For Key-Management Scheme For Use With Internet Protocols at Site Firewalls". This system consists of separate private networks which communicate over an Internet type connection through firewalls. A private network "I" communicates through a firewall "A" to the Internet where the message is transferred to firewall "B" and then decoded and sent on to another private network "J". This allows private network "I" and private network "J" to communicate in a secure encapsulated message while having firewall protection. The invention begins with a source node "I" sending a data gram to the firewall "A". Firewall "A" has a secret value "SA" and a public value "PA". Similarly, firewall "B" is provided with a secret value "SB" and a public value "PB". In this manner both firewall "A" and firewall "B" can acquire a shared secret value "SAB" without having to communicate. The communication is initiated by providing firewall "A" and firewall "B" with initial values for all other secure firewalls on the network. Firewalls "A" and "B" then use secret value "SAB" to create a key "KAB". The transmitting firewall then generates a random key "KP" which is used to encrypt the received data. The key "KP" and the encrypted data are then all encrypted by the public key "KAB" for transmission over the Internet. Firewall "B" will then use key "KAB" to de-crypt the message for the private key "KP" and de-crypt the data that has been transmitted. In this manner the transmitting firewall can constantly be changing the private key "KP" which increases the security of the system.

The above-described key distribution and encryption systems suffer from the drawbacks of using known communication pathways, having known addresses, and some systems even transfer secure key information over the communication lines.

Hence, there is a need for an improved communication method which allows for encrypted information transfer to dynamic locations without transmitting the keys over the communication line.

Additionally, there remains a need for a mechanism in which to log on to a computer system securely without passing password.

BRIEF SUMMARY OF THE INVENTION

In accordance with the present invention, an improved encoded or encrypted method for transferring information is provided which addresses the drawbacks of the prior art devices.

In accordance with one embodiment of the present invention a message is input to a first device which obtains a dynamic address from a first server to allow for connection to a second server.

A further embodiment of the invention allows for transmitting the message from the first device to the second server, receiving the message at the second server, storing the message until transfer to a second device as requested, and then transmitting the message to the second device from the second server.

Another embodiment of the present invention allows for encoding the message before it is input to the first device, and decoding the message after it has been received at the second device.

Yet another embodiment of the present invention allows for multiple servers which can be contacted to obtain the dynamic address of another server.

A still further embodiment of the present invention uses a remote administrator to control access both to the first server for obtaining the dynamic addresses, and to the second server for message transfers.

In accordance with another embodiment of the present invention, the user access to the secure name server is controlled by a remote administrator which creates, authorizes and deletes valid user ID/password combinations.

In accordance with another example of the present invention, the system allows for an electronic mail transfer between two users where a direct communication between the first user and second user never occurs. In this manner, two users can communicate without actually having a direct connection which is detectable by other parties.

The principal object of the present invention is to provide an easy to use, protected, electronic mail system for communication.

Another object of the present invention is to allow for the establishment of multiple electronic mail servers for different user categories.

A still further object of the present invention is to provide for a system which can communication on both secure and non-secure electronic mail servers.

Yet another object of the present invention is to provide for a program which allows for automatic and immediate deletion of electronic mail messages once they have been sent.

Other objects and further scope of the applicability of the present invention will become apparent from the detailed description to follow, taken in conjunction with the accompanying drawings wherein like parts are designated by like reference numerals.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic view of a network communication arrangement utilizing a secure electronic mail system of the present invention.

FIG. 2 is a flow chart representation of the process to remotely administrate electronic mail accounts.

FIG. 3 is a flow chart representation of the process used to send mail.

FIG. 4 is a flow chart representation of a process used to retrieve mail.

FIG. 5 is a flow chart representation of a process to register a machine with a secure name server.

FIG. 6 is a flow chart representation of a process for obtaining an IP address from alternate secure name servers.

FIG. 7 is a flow chart representation of a process to get an IP address from a particular secure name server.

FIG. 8 is a flow chart representation of a connection process to a secure electronic mail server.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In accordance with one exemplary embodiment of the present invention as shown in FIG. 1, a protected communication network is generally designated by the reference numeral 10.

In the preferred embodiment, the protected communication network 10 consists of a first central processing unit or user 12, a secure name server 14, a secure electronic mail server 16, a second central processing unit or user 18, a remote administrator 20 and a connecting network 22. The general operation of the overall system will be outlined in the following discussion.

Initially, the secure electronic mail server 16 will establish a link to a connecting network 22 and obtain a dynamic address. The dynamic address is standardly assigned by the network to a user of the network. An example of a dynamic address is a dynamic Internet protocol address for communicating over the Internet or world wide web. The secure electronic mail server 16 will then contact the secure name server 14 which has a fixed address on the connecting network 22. The secure electronic mail server 16 will then notify the secure name server 14 of the secure electronic mail server's 16 dynamic address on the connecting network 22. The communication between the secure electronic mail server 16 and the secure name server 14 will then be discontinued.

It will be understood that the present invention will be applicable to various types of networks.

Next, the remote administrator 20 will log on to the connecting network 22 and communicate with the secure name server 14. Note that this communication is a protected communication to allow for a protected information transfer. The secure name server 14 transfers the dynamic address of the secure electronic mail server 16 to the remote administrator 20. The communication between the secure name server 14 and the remote administrator 20 is then discontinued.

In an alternate embodiment, the remote administrator 20 will establish logon protocol for users to access the secure name server 14. The remote administrator 20 will then have the information to pass on to users of the protected communication network 10 to allow them to access the secure name server 14 through their logon protocol. In this manner, access to the secure name server 14 is controlled by the logon protocol, and only users authorized by the remote administrator 20 will be allowed to access the secure name server 14.

After receiving the dynamic address of the secure electronic mail server 16, the remote administrator 20 will initiate a communication with the secure electronic mail server 16 over the network 22. Once again, this is a protected information transfer communication. During this communication, the remote administrator 20 will create, change, and delete authorized user ID/password combinations for accessing the secure electronic mail server 16. The

communication between the remote administrator 20 and the secure electronic mail server 16 will then be discontinued.

As different users require access to the system, the remote administrator 20 will provide the appropriate logon protocol and/or authorized ID/password combinations to the users to allow for access to the protected communication network 10. In this example, both the first user 12 and the second user 18 contact the remote administrator 20 for authorized logon protocol and user ID/password combinations.

The first user 12 now wishes to write and send an electronic mail communication to the second user 18 over the protected communication network 10. The first user 12 uses his unique logon protocol combination to access the secure name server 14 over the connecting network 22. Once again, this is a protected communication. The first user 12 then obtains the dynamic address of the secure electronic mail server 16 from the secure name server 14. The communication between the first user 12 and the secure name server 14 is then discontinued.

The first user 12 now uses his ID/password combination and the dynamic address to log onto the secure electronic mail server 16. Once the first user 12 has logged on to the secure electronic mail server 16, the first user's 12 electronic mail message is then protected by a protection method, such as encryption, and sent on the communication network 22 to the designated recipient's box on the secure electronic mail server 16. In this example, the information would be stored in the second user's box. The communication between the first user 12 and secure electronic mail server 16 is then broken.

periodically

At random intervals, the second user 18 will use his separate logon protocol to obtain the dynamic address of the electronic mail server 16 from the secure name server 14 and then access the secure electronic mail server 16 with his ID/Password combination to see if 20 there are messages for the second user 18. If there are messages in the second user's box on the secure mail server 16, the secure electronic mail server 16 will notify the second user 18 that there are messages available for retrieval. The secure electronic mail server 16 will then use a protected transfer to send the electronic mail message from the first user 12 to the second user 18 over the connecting network 22. The communication between the second user 18 and the secure electronic mail server 16 is then discontinued. Thus, a message has been transferred from the first user 12 to the second user 18 without a direct connection between the first user 12 and the second user 18.

It will also be understood that, in an alternate arrangement, the secure name server and the secure mail server may reside on the same computer system.

The aforementioned method of communication provides several levels of communication protection against outside interference for unwanted monitoring.

First, the first user 12 and the second user 18 never communicate directly. Thus, an outside person must monitor multiple communication pathways to detect communication between the first user 12 and the second user 18.

Second, because the secure electronic mail server uses a dynamic address, the communication pathways to and from the secure electronic mail server 16 are constantly changing. This increases the difficulty of monitoring communication with the secure electronic mail server 16.

Third, because the dynamic address of the secure electronic mail server 16 must be obtained from the secure name server 14, the address of the secure name server 14 must be known.

Fourth, because the secure name server 14 requires a proper log protocol combination, the dynamic address of the secure electronic mail server 16 is not easily obtained.

Fifth, because the secure name server 14 transfers the dynamic address of the secure electronic mail server 16 in an encrypted message, a first level of encryption must be broken just to obtain the dynamic address for the secure electronic mail server 16.

Sixth, because a communication between a user and the secure mail server 16 is protected, a second level of encryption must be broken to obtain the message.

Seventh, because the users can be using an additional protection or encryption system that is unknown to the secure networks, an additional level of protection can be used between the first user 12 and the second user 18. This additional level must also be broken to obtain the message text.

Eighth, because the entire system is controlled by a remote administrator 20, logon protocols, passwords, and keys can be constantly updated and changed. Any compromised logon protocol or ID/password combinations can be immediately deleted from the system by the remote administrator 20.

In addition, multiple applications of the present system could provide for a system where the communication between the remote administrator 20 and a secure electronic mail server 16 would also be an indirect communication through another electronic mail server 16.

While these descriptions of protection levels illustrate one example of the present invention, it is to be understood that the different levels of protection or additional levels of protection may be implemented in conjunction with the present invention to further enhance security.

The sub-processes for communicating throughout the network include the process to administrate electronic mail accounts, the process to send electronic mail, the process to retrieve mail, the process to register a machine with a secure name server, the process to obtain a dynamic address from alternate secure name servers, the process to get an address from a secure name server, and the process to connect to a secure electronic mail server.

Each of the sub-processes for communicating will be given further detail in the following discussion.

Process to Administrate Electronic Mail Accounts

FIG. 2 of the drawings outlines the process by which the remote administrator sets up the user ID/password combinations. The process starts 30 by initializing the parameters necessary for operation of the process. The system will then check a first secure name server 32 for the dynamic address of the secure mail server. Block 34 represents the system checking to see it properly obtained the dynamic address of secure mail server from the first secure name server. If the system is successful in obtaining the secure mail server dynamic address from the first secure name server, the system will move on connect to the mail server as shown at block 36.

If the system is not successful in obtaining the dynamic address of the secure mail server from the first name server as shown in block 34, the system will move on to attempt to obtain the dynamic address of the secure mail server from the second secure name server, as shown in block 48. As shown in block 50, the system will check to see if it has now successfully retrieved the secure mail server dynamic address from the second secure name server. If the system is

successful then the system will move on to connect to the secure mail server as shown in block **36**. If the system has not successfully obtained the dynamic address of the secure mail server from either the first name server or the second secure name server the system will send back a report error as shown in block **52** and return an error code to the user as shown in block **54**.

If the system has successfully obtained the dynamic address of the secure mail server, it will connect to the secure mail server using the dynamic address as shown in block **36**. The remote administrator will then be able to add user ID/passwords as shown in block **38**, modify user ID/passwords as shown in block **40**, and delete user ID/passwords as shown in block **42**. The remote administrator will then disconnect from the secure mail server as shown in block **44**. The system will then end the process to remotely administrate as shown in block **46**.

A similar process could be adapted to change the logon protocol for the secure name servers.

Process Used to Send Electronic Mail

FIG. **3** of the drawings outlines the process by which the secure electronic mail programs send mail communications. The process will start **60** by initializing the parameters necessary for operation of the process. The user will then use his logon protocol to check a first secure name server **62** for the dynamic address of the secure mail server. Block **64** represents checking to see it properly obtained the dynamic address of secure mail server **20** from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server, the user will move on connect to the mail server at block **66**.

If the system is not successful in obtaining the dynamic address of the secure mail server from the first name server as shown in block **64**, the system will move on to get the dynamic address of the secure mail server from the second secure name server, as shown in block **74**. As shown in block **76**, the user will check to see if it has now successfully retrieved the secure mail server dynamic address from the second secure name server. If the user is successful, then the user will move on to connect to the secure mail server as shown in block **66**. If the user has not successfully obtained the dynamic address of the secure mail server from either the first name server or the second secure name server, the user will send back the report error as shown in block **78** and return the error code to the operator as shown in block **80**.

If the user has successfully used its logon protocol to obtain the dynamic address of the secure electronic mail server, it will connect to the secure mail server using the dynamic address as shown in block **66**.

Once the user has successfully connected to the electronic mail server, the electronic mail is protected and sent to the electronic mail server as shown at block **68**. The user then disconnects from the secure electronic mail server as shown at block **70**, and ends the process as shown at block **72**.

Process Used to Retrieve Mail

FIG. **4** of the drawings outlines the process by which a user retrieves mail from the secure mail server. The process will start **90** by initializing the parameters necessary for operation of the process. The user will use its logon protocol to check a first secure name server **92** for the dynamic address of the secure mail server. Block **94** represents the user checking to see it properly obtained the dynamic address of secure mail server from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name server, the user will move on connect to the mail server at block **96**.

If the user is not successful in obtaining the dynamic address of the secure mail server from the first name server as shown in block **94**, the user will move on to get the dynamic address of the secure mail server from the second secure name server, as shown in block **110**. As shown in block **112**, the user will check to see if it has now successfully retrieved the secure mail server dynamic address from the second secure name server. If the user is successful, then the system will move on to connect to the secure mail server as shown in block **96**. If the system has not successfully obtained the dynamic address of the secure mail server from either the first name server or the second secure name server, the user will send back the report error as shown in block **116** and return the error code to the user as shown in block **118**.

Once the user or retrieval program has properly connected to the electronic mail server, the electronic mail program will check to see if mail is available as shown in block **98**.

If mail is available in block **98**, then the retrieval program will retrieve the message headers as shown in block **100**, retrieve the selected message as shown in block **102**, delete the message from the secure mail server as shown in block **104**, and disconnect from the secure electronic mail server as shown in block **106**. The retrieval program will then restore the necessary parameters to properly end this process as shown in block **108**.

If it is detected in block **98** that mail is not available, the retrieval program will disconnect from the secure mail server as shown in block **114**.

Process to Register Machine with a Secure Name Server

As shown in FIG. **5**, when a user, administrator, or secure electronic mail server logs onto the system with a dynamic address, the secure name server is contacted. The process for establishing this connection and supplying the proper dynamic address to the secure name server is outlined as follows.

As shown in block **120**, the registering CPU machine selects an appropriate secure name server to be contacted. The registering machine then supplies the secure name server with these proper logon protocol combination as shown in block **122**. As shown in block **124**, a session with a secure name server is then established. If the session is successfully established as shown in block **126**, then the machine will go on to register the dynamic address for the named machine **128**, disconnect the session **130**, and then properly shut down this process as shown in block **134**.

If the session was not properly established in block **126**, then the machine will report an error to the user or operator at block **136**, and return an error code as shown in block **138**.

Process to Obtain a Dynamic Address from Alternate Secure Name Servers

FIG. **2** of the drawings outlines the process by which a network user obtains a dynamic address from multiple secure name servers. The network user will use his logon protocol to check a first secure name server **140** for the dynamic address of the secure mail server. Block **141** represents the user checking to see it properly obtained the dynamic address of secure mail server from the first secure name server. If the user is successful in obtaining the secure mail server dynamic address from the first secure name

server, the system will return the dynamic address to the user program as shown at block **142**.

If the user is not successful in obtaining the dynamic address of the secure mail server from the first name server as shown in block **141**, the user will move on to get the dynamic address of the secure mail server, from the second secure name server, as shown in block **143**. As shown in block **144**, the user will use its logon protocol to check to see if it has now successfully retrieved the secure mail server dynamic address from the second secure name server. If the user is successful then the system will return the dynamic address to the user program as shown in block **142**. If the user has not successfully obtained the dynamic address of the secure mail server from either the first name server or the second secure name server, the system will send back the report error as shown in block **145** and return the error code to the user as shown in block **146**.

Process to Get an Address from a Secure Name Server

FIG. **7** of the drawings outlines the process by which an unknown address, such as the dynamic address of a secure mail server, is obtained from a secure name server. The process starts by selecting the target secure name server machine by its fixed address/name as shown in block **150**. The user then provides the secure name server with its logon protocol combination as shown at block **152**. If the user logon combination is verified then a session is established with a secure name server as shown at block **154**. As shown at block **156**, if the session has not been correctly established then the secure name server will report an error code as shown at block **178** and return the error code to the user as shown at block **180**.

Returning to block **156**, if the session has been correctly established as shown at block **156**, then the user will be allowed to request the address for the named machine at the client site as shown at block **158**.

The system will then perform a series of checks to see if the named machine has been properly identified. If the named machine has not been properly identified, shown at block **160**, then the system will be disconnected as shown at block **172**, move on to reporting the error code as shown at block **178**, and continue processing.

If the named machine has been properly defined as shown at block **160**, then the system will check to see if the named machine has properly registered its address shown at block **162**. If the address has not been correctly registered, then the system will move on to disconnect session as shown at block **174**, report the error code as shown at block **178**, and continue processing. If the named machine has properly registered its address as shown at block **162**, then the machine will check to see if the registration is up to date as shown at block **164**.

If the registration is not properly up to date as shown at block **164**, then the system will disconnect the session as shown at block **176**, move on to report the error code as shown at block **178**, and continue processing.

If the system registration has been properly updated as shown at block **164**, then the system will return the obtained address as shown in block **168** and disconnect the session as shown in block **166**. The system will then end processing as shown at block **170**.

Process to Connect to Secure Electronic Mail Server

FIG. **8** of the drawings outlines the process by which a connection to a secure electronic mail server is made. The process begins by the user selecting the secure electronic mail server using the current dynamic address as shown at block **190**. The user will then provide the user ID/password combination for the target secure mail server as shown at block **192**. The user will then attempt to establish a session with secure electronic mail server as shown at block **194**. The system will check to make sure that the session has been correctly established as shown at block **196**.

If the session has been correctly established as shown at block **196**, then the system will return to processing as shown at block **198** and allow the user to continue.

If the communication session has not been correctly established as shown at block **196**, then the system will report an error as shown at block **200** and forward the error back to the user as shown at block **202**.

The preferred embodiment of the present invention uses multiple secured name servers to allow for access to the secure mail server. However, it is also envisioned that a single secure name server or additional secure name servers could be used with this invention. It is also envisioned that the secure name server and the secure mail server could reside on the same machine. In this manner, two separate communication lines would be necessary to allow for the fixed address of the secure name server while providing for a dynamic address of the secure mail server.

It is also envisioned that the logon combination and user ID/password combination could be identical.

While the foregoing detailed description has described several embodiments of the secure electronic mail system in accordance with this invention, it is to be understood that the above description is illustrative and not limiting of the disclosed invention.

The claims and the specification describe the invention presented and the terms that are employed in the claims draw their meaning from the use of such terms in the specification. The same terms employed in the prior art may be broader in meaning than specifically employed herein. Whenever there is a question between the broader definition of such terms used in the prior art and the more specific use of the terms herein, the more specific meaning is meant.

While the invention has been described with a certain degree of particularity, it is manifest that many changes may be made in the details of construction and the arrangement of components without departing from the spirit and scope of this disclosure. It is understood that the invention is not limited to the embodiments set forth herein for purposes of exemplification, but is to be limited only by the scope of the attached claim or claims, including the full range of equivalency to which each element thereof is entitled.

What is claimed is:

1. A method for transferring messages on a computer network, comprising:

encoding a message;

inputting said message to be transmitted at a first device;

encrypting said message at said first device;

retrieving an address for a dynamically addressed mail server by contacting a first secure name server separate from said mail server using a unique combination ID/password to retrieve said dynamic address;

connecting said first device to said mail server using said server dynamic address;

transmitting said encrypted message from said first device to said mail server;

receiving said message at said mail server;

transmitting said message from said mail server to a second device;

decrypting said message at said second device; and

decoding said message.

2. The method of claim 1, wherein obtaining an address for the dynamically addressed mail server further comprises:

contacting a second name server upon a failure to obtain the address from said first secure name server.

3. The method of claim 1, further comprising:

automatically deleting the message after transmitting the message from said dynamically addressed mail server.

4. A method for transferring messages on a computer network, comprising:

establishing a link between an electronic mail server and a network;

retrieving a dynamic address for said electronic mail server from a separate secure name server using a unique combination ID/password;

establish a communication with said electronic mail server across said network;

notifying said secure name server of said dynamic address of said electronic mail server; and

thereafter discontinuing said communication between said electronic mail server and said secure name server.

5. The method for transferring messages on a computer network of claim 4, further comprising:

establishing communication between a remote administrator and said secure name server on said network;

transferring said dynamic address of said electronic mail server from said secure name server to said remote administrator;

discontinuing said communication between said secure name server and said remote administrator.

6. The method for transferring messages on a computer network of claim 5, further comprising:

establishing a communication between said remote administrator and said secure electronic mail server across said network;

updating ID/password combinations for accessing said secure electronic mail server;

discontinuing said communication between said remote administrator and said secure electronic mail server.

7. The method of claim 6, further comprising:

distributing said ID/password combinations to users of said network.

8. The method of claim 7, further comprising:

establishing a communication between a first user and said secure name server using a first unique ID/password combination;

transmitting said dynamic address of said secure electronic mail server to said first user from said secure name server;

discontinuing said communication between said first user and said secure name server.

9. The method of claim 8, further comprising:

establishing a connection between said first user and said secure electronic mail server;

encrypting a message from said first user;

transferring said message from said first user to said secure electronic mail server across said network;

discontinuing the communication between said first user and said secure electronic mail server.

10. The method of claim 9, further comprising:

monitoring said secure electronic mail server by a second user;

notifying said second user that a message is waiting for said second user;

transferring said message from said secure electronic mail server to said second user;

discontinuing said connection between said second user and said electronic mail server.

11. A method for transferring messages on a computer network, comprising:

establishing a link between an electronic mail server and a network;

retrieving a dynamic address for said electronic mail server from a separate secure name server using a unique combination ID/password;

establishing a communication with said electronic mail server across said network;

notifying said secure name server of said dynamic address of said electronic mail server;

thereafter discontinuing said communication between said electronic mail server and said secure name server;

establishing a communication between a first user and said secure name server using a first unique combination ID/password;

transmitting said dynamic address of said secure electronic mail server to said first user from said secure name server; and

discontinuing said communication between said first user and said secure name server.

* * * * *